SPECTRUM Software Release Notice (SSRN)

For SPECTRUM 6.6 with Service Pack 5 CD release

Document 5156

APRISMA SPECTRUM® POWERED SOLUTIONS

Notice

Copyright Notice Copyright © 2004-present by Aprisma Management Technologies, Inc. All rights reserved worldwide. Use, duplication, or disclosure by the United States government is subject to the restrictions set forth in DFARS 252.227-7013(c)(1)(ii) and FAR 52.227-19.

Liability Disclaimer Aprisma Management Technologies, Inc. (“Aprisma”) reserves the right to make changes in specifications and other information contained in this document without prior notice. In all cases, the reader should contact Aprisma to inquire if any changes have been made.

The hardware, firmware, or software described in this manual is subject to change without notice.

IN NO EVENT SHALL APRISMA, ITS EMPLOYEES, OFFICERS, DIRECTORS, AGENTS, OR AFFILIATES BE LIABLE FOR ANY INCIDENTAL, INDIRECT, SPECIAL, OR CONSEQUENTIAL DAMAGES WHATSOEVER (INCLUDING BUT NOT LIMITED TO LOST PROFITS) ARISING OUT OF OR RELATED TO THIS MANUAL OR THE INFORMATION CONTAINED IN IT, EVEN IF APRISMA HAS BEEN ADVISED OF, HAS KNOWN, OR SHOULD HAVE KNOWN, THE POSSIBILITY OF SUCH DAMAGES.

Trademark, Service Mark, and Logo Information SPECTRUM, IMT, and the SPECTRUM IMT/VNM logo are registered trademarks of Aprisma Management Technologies, Inc., or its affiliates. APRISMA, APRISMA MANAGEMENT TECHNOLOGIES, the APRISMA MANAGEMENT TECHNOLOGIES logo, MANAGE WHAT MATTERS, DCM, VNM, SpectroGRAPH, SpectroSERVER, Inductive Modeling Technology, Device Communications Manager, SPECTRUM Security Manager, and Virtual Network Machine are unregistered trademarks of Aprisma Management Technologies, Inc., or its affiliates. For a complete list of Aprisma trademarks, service marks, and trade names, go to:

http://www.aprisma.com/manuals/trademark-list.htm

All referenced trademarks, service marks, and trade names identified in this document, whether registered or unregistered, are the intellectual property of their respective owners. No rights are granted by Aprisma Management Technologies, Inc., to use such marks, whether by implication, estoppel, or otherwise. If you have comments or concerns about trademark or copyright references, please send an e-mail to spectrum-docs@aprisma.com; we will do our best to help.

Restricted Rights Notice (Applicable to licenses to the United States government only.)
This software and/or user documentation is/are provided with RESTRICTED AND LIMITED RIGHTS. Use, duplication, or disclosure by the government is subject to restrictions as set forth in FAR 52.227-14 (June 1987) Alternate III(g)(3) (June 1987), FAR 52.227-19 (June 1987), or DFARS 52.227-7013(c)(1)(ii) (June 1988), and/or in similar or successor clauses in the FAR or DFARS, or in the DOD or NASA FAR Supplement, as applicable. Contractor/manufacturer is Aprisma Management Technologies, Inc. In the event the government seeks to obtain the software pursuant to standard commercial practice, this software agreement, instead of the noted regulatory clauses, shall control the terms of the government's license.

Virus Disclaimer Aprisma makes no representations or warranties to the effect that the licensed software is virus-free. Aprisma has tested its software with current virus-checking technologies. However, because no antivirus system is 100-percent effective, we strongly recommend that you write protect the licensed software and verify (with an antivirus system with which you have confidence) that the licensed software, prior to installation, is virus-free.

Contact Information Aprisma Management Technologies, Inc., 273 Corporate Drive, Portsmouth, NH 03801 USA

Phone: 603.334.2100
U.S. toll-free: 877.468.1448
Web site: http://www.aprisma.com

Contents

Notice **2**

Overview **7**

Upgrade Considerations **8**

SPECTRUM 6.6 Feature List **14**

AutoDiscovery 14
Performance 14
Accuracy 15
Smart Defaults 15
General Usability 16
Distributed Install 17
Event and Alarm Management 17
Maintenance Mode 17
MPLS Manager 18
Mulitcast Manager 19
New Management Modules 20
Enhanced Management Modules 24
Non-Persistent Connection Manager (NPC) 26
Process Daemon 26
Service Performance Manager (SPM) 27
SPECTRUM Reporting Gateway 27
SNMPv3 28
SPECTRUM Configuration Manager 28
Trap Handling 28
Web Operator Suite 29
VPN Manager 30
Performance 31
Additional Usability Enhancements 31
Miscellaneous Enhancements 32

Corrected Issues 33
ATM Manager 33
AutoDiscovery & Modeling 33
CLI 34
Database, Data Export, & Reports 35
Event & Alarm Management 36
Fault Tolerance 37
Installation 38
Location Server 38
Miscellaneous 39
Management Modules 40
Dominion Web Reporter 42
Search Manager 43
Security 43
SpectroGraph 43
SpectroSERVER 45
Toolkits 46
Web Operator Suite 46

Known Anomalies in SPECTRUM 6.6 with Service Pack 5 CD Release 47
AR System Gateway 47
Enterprise Alarm Manager (EAM) 48
Level I Developer's Toolkit 49
SpectroSERVER 50
SPECTRUM Installation/Uninstallation Programs 50
Cabletron SmartSwitch 6000 Family 51
Cabletron SmartSwitch 9000/9500 52
Cisco Catalyst 54
Cisco Router 55
Empire Agent 56
Enterasys Matrix E5 57
Extreme Devices 58

F5 Networks 59
ForeRunner Series of ATM Switches 59
Host Compaq Module 60
Juniper Networks 61
Packeteer PacketShaper 62
Nortel Contivity Extranet Switch 62
Riverstone SmartSwitch Router 63
SmartSwitch Routers (SSR) 64
Sun Management Center Agent 65
SynOptics 5000 Hubs 66
SynOptics Modules 67
Wellfleet Routers 68
Multiple Management Modules 69

Discontinued Products and Components 70
About Discontinued Products and Components 70
Device Management Components 71
Cabletron Device Management Components 71
Management Modules 72
Questions & Answers 72
Feature Comparison 73
EPI, SSAPI, IHAPI, Simulator Playback Tool 76
Questions & Answers 76
Feature Comparison 78
SpectroRX 79
Questions & Answers 79
Feature Comparison 79
Support for Export to SAS, Ingress, Sybase, Oracle, and Microsoft SQL Database Types 80
Questions & Answers 80
Feature Comparison 81
Support for Netscape 82
Questions & Answers 82

Feature Comparison 83

Index 84

Overview

A copy of this SPECTRUM Software Release Notice (SSRN) is included on both the SPECTRUM Application CD Version 6.6 with Service Pack 5 and the SPECTRUM Documentation CD Version 6.6 with Service Pack 5; it is also available online at http://www.aprisma.com/manuals.

This SSRN is intended to alert users to special considerations for upgrades, product enhancements or changes, late-breaking information, and corrected and known anomalies.

It is strongly recommended that you read this SSRN so you are aware of any changes in the product or the associated documentation.

Upgrade Considerations

This section identifies product changes that should be considered when upgrading from prior releases. Some of these changes may require modifications to existing SPECTRUM customizations and integrations.

Note: The SPECTRUM Application CD Version 6.6 with Service Pack 5 may not be used to upgrade an existing 6.6 SPECTRUM installation. Instead, upgrade using the Service Pack 5 downloadable version available at http://www.aprisma.com/support/secure/download/.

- In SP5, the format of backup files created with ddm_save has been changed. Instead of a proprietary format, the backup files produced by ddm_save are now simply gzip'ed tar files of the key DDMDb database data files needed to recreate a DDMDb database. This change should be transparent to most customers. However, customers who have built scripting dependent on the name of files created by ddm_save may need to adapt their scripts to allow for the new default file extension ".tgz" that will be appended to the file name. Note that ddm_load supports both the original proprietary save file format and the new file format and automatically distinguishes between them.
- SPECTRUM now comes pre-configured with ports 14001-14005 assigned to certain SPECTRUM processes. Any firewall must be configured to allow bi-directional UDP traffic for ports 14000 and 14001 and bi-directional TCP traffic for ports 14002-14005. If you had previously customized your environment by changing the OSAGENT_PORT from its default of 14000 to any of the ports in the range 14001-14005, then a required SPECTRUM process may not run. To correct this situation, choose a different available UDP port for the OSAGENT_PORT setting.
- If you are using SPECTRUM Web Operator and if you have made changes to the WebApps/tomcat/webapps/spectrum/WEB-INF/web.xml file, your changes to that file will need to be re-applied after installing 6.6 with SP5 CD release.
- A new post-installation script has been introduced, to allow customers to easily convert existing device models from the general GnSNMPDev model type, to a more specific device model type appropriate for the

device. Please refer to the "Converting Eligible GnSNMPDev Models to New Model Types" section of the "SPECTRUM Installation Guide (6.6 Service Pack Release)" (5136.pdf) for more details.

- If you are managing Motorola Vanguard or Cisco/Stratacom IGX devices, and you are using SPECTRUM ATM Circuit Manager and/or SPECTRUM Frame Relay Manager, your existing device models must be updated. This can be accomplished by manually destroying and re-creating any Motorola Vanguard or Cisco/Stratacom IGX device models. If you have a large number of these device models, then you may choose to contact Aprisma Support to obtain a script (AdvApp_Migration) that can be run to perform this conversion/update automatically.
- Many improvements have been made to Live Pipes, Port Status Polling, and Link Trap Handling. Any customer making use of these features, should review this section carefully, and read the new "Configuring Port Status Monitoring" section of the "How To Manage Your Network with SPECTRUM" guide for further details.
  - Live Pipes Polling Criteria: Historically, if both ports involved in a Live Pipe have Polling_Status set to False and Polling_Interval set to 0, then the link condition would be evaluated every 60 seconds automatically. Now, the following criteria must be met in order for the status of a port to be polled:
    - The Polling_Status (0x1154f) of the port model must be TRUE.
    - The Polling_Interval (0x10071) of the port model must be non-zero.
    - The Polling_Status of the port's device model must be TRUE.
    - The device model must not be in Maintenance Mode.
    - The port model must not be in Maintenance Mode.
  - PollPortStatus Change: The PollPortStatus attribute on device models now functions differently. Previously, this attribute was just used to set the PollPortStatus attribute on all the ports of the device. Now, this attribute controls whether the port models (whose PollPortStatus attribute is set to TRUE) will be polled or not. For a port to be polled, both the device's PollPortStatus attribute (0x12809) and the port's PollPortStatus attribute(0x1280a) must be TRUE.

Important: SPECTRUM no longer uses a default polling interval of 60 seconds for this feature if the port's Polling_Interval is 0 (zero). If zero, the status of the port is not polled.

- Wide Area Link Monitoring: The statuses of ports connected to a WA_Link model are automatically polled, and this is controlled by the Polling_Status and Polling_Interval of the WA_Link model. If the WA_Link model's Polling_Status is TRUE, and its Polling_Interval is non-zero, SPECTRUM will automatically make the pipes connected to a WA_Link "live." This allows the user to visually verify that SPECTRUM is, in fact, monitoring the status of the connected ports. In previous versions of SPECTRUM, the user was not aware that this polling occurred, unless they read the documentation. Users still have full control of the pipe, and can turn it off and on after the connection is made. SPECTRUM no longer uses the Polling_Interval of the WA_Link model to determine how often to poll the status of the connected ports. It now uses each individual port model's Polling_Interval, which most likely was inherited from the device model, but may be customized on a per-port basis.

- New fault handling functionality was added to the WA_Link model to allow more user control and flexibility. A new attribute called LinkFaultDisposition (0x129e2) has been created in the WA_Link model type, which supports three different modes: 0 = BothPortsAndLink, 1 = PortsOnly, 2 = LinkOnly. When a wide area connection goes down, alarms could be generated on ports and/or the link model. If this attribute is set to BothPortsAndLink, then alarms will be generated on both the connected ports and the link model. If this attribute is set to PortsOnly, then only the connected ports will be alarmed, and the WA_Link will be suppressed. If this attribute is set to LinkOnly, then only the WA_Link model will be alarmed, and the ports will be suppressed. The new attribute is accessible via the WA_Link model's new Fault Management GIB, or using the Global Attribute Editor. The default setting for LinkFaultDisposition is BothPortsAndLink (0), which preserves pre-6.6 alarm behavior.

- Port Criticality: SPECTRUM users can now assign a relative "importance" to port models since ports now have the Criticality (0x1290c) attribute. The Criticality of a port is not currently used in any Impact Severity calculations, but users can display the Criticality of a port in the Alarm View to allow prioritization of port alarms. Additionally, the Criticality attribute has been added to the port

model's Fault Management GIB, and can now be set using the Global Attribute Editor.

- Link Trap Handling: Historically, SPECTRUM handled Link Down and Link Up traps by simply generating an event and a red alarm on the port model to which the trap corresponds. Additionally, an event and yellow alarm will be generated on the device model. These events and alarms were not integrated with other port status monitoring functionality. As a result, a SPECTRUM user may see two red alarms for the same problem (a port went down).one alarm resulting from the Link Down trap, and another resulting from Live Pipes or PollPortStatus intelligence. Now, a link down trap will merely initiate an evaluation of the port's status by the regular port status intelligence (provided the AlarmOnLinkDownTrap attribute is set to ALWAYS or CHECK ADMIN). SPECTRUM still generates a yellow alarm on the device model to allow easy access to vendor-specific trap data; however we no longer generate the trap-specific events and alarms on the affected port model. Here is a list of the events and alarms that are no longer generated, and the events and alarms that replace them. Any customer with a possible dependence on the specific Events/Alarms generated from Link Traps should review that table and adjust any dependent processing to use the new Events/ Alarms.

Event Description	**Event**	**Alarm Description**	**Alarm Id**	**New Event/ Alarm**
Port status transitioned to "down"	0x10d73	THE COMMUNICATION LINK IS DOWN	0x220002	0x10D11/ 0x1040a
Port status transitioned to "down", but is administratively "off".	0x10d74	THE COMMUNICATION LINK IS DOWN	0x220002	0x10d12/ 0x1040b
Port status transitioned to "down" because lower layer is down.	0x10d75	THE LOWER LAYER COMMUNICATION LINK IS DOWN	0x220006	0x10d16/ 0x1040f
Port status transitioned to "up"	0x10d76	N/A	N/A	0x10d10/ N/A

- SPECTRUM no longer polls the status of a port for which it's received a LinkDown trap, to monitor when it comes back up. This was done for performance and consistency reasons. If the user wants the status of a port polled, they can make the pipe connected to it "live," or set PollPortStatus on the port model to TRUE. Note that Cisco devices running pre-12.0 IOS will not send a LinkUp trap, and therefore enabling a Live Pipe or PollPortStatus on links/interfaces of interest would be required to get automatic LinkDown alarm clearing.
- Automatic Alarm Clearing: It is important to note that any port status alarm will be automatically cleared by SPECTRUM if both of the port's ok_to_poll and PollPortStatus attributes are set to FALSE.

- Warning message(s) may occur in the install log. These warnings do not imply a problem and can be ignored. For example: "Warning: Attribute 0x114e2 does not appear to be a valid attribute for modeltype 0xXXXXXXX. Default value not set."
- AlarmNotifier will only pass the most recent event for an alarm update if the new SHOW_ALL_EVENTS .alarmrc parameter is set to FALSE. By default, this new parameter is set to FALSE, thereby changing the out-of-box behavior of AlarmNotifier. For AlarmNotifier integrations that depend on the prior default behavior of all associated events being passed with alarm updates, SHOW_ALL_EVENTS should be set to TRUE in the .alarmrc.
- CLI output change - CLI "show attributes" output for multiple attributes are now reported in the same order as they were requested. This restores the behavior that existed prior to the 6.5.1 release. (*** This may require certain CLI scripts to be adapted to support this output change.)
- AutoDiscovery behavior change - When you run a container based discovery (with Map Topology unchecked), AutoDiscovery now attempts to move all models (both new and pre-existing) that correspond to entries in the result set into the chosen container. Previously, a container-based discovery (with Map Topology unchecked) would only put new models in the container. The current work-around is to set the IsMovable attribute to FALSE for all existing device models before performing any container-based discoveries. To do this using Search Manager (for device models selected from search results), select Management > Set Attribute Values and set Topologically Relocate Models to False.

- The AutoDiscovery application database, which stores configurations and result sets, has been re-implemented. The first time Auto Discovery is run after upgrading to this 6.6 SP5 CD release, the pre-existing database will be automatically converted to the new implementation, preserving any pre-existing data. As an added precaution, the installation will copy the entire pre-existing SPECROOT/AutoDiscover directory to SPECROOT/AutoDiscover.backup. Once the new version of Auto Discovery has been run successfully, and access to any pre-existing data has been verified, the SPECROOT/AutoDiscover.backup directory can be safely removed.
- The JMibTools application database, which stores compiled SNMP MIB information, has been re-implemented. The first time JMibTools is run after upgrading to this 6.6 SP5 CD release, the pre-existing database will be automatically converted to the new implementation format, preserving any previously imported MIB data. This process will cause a noticeable delay the first time JMibTools is run. Subsequent runs will not suffer from this one-time database conversion delay.
- A number of Attributes in the Cisco_IP_MIB Model Type were re-created with the correct data type (IP Address) to avoid a potential SpectroSERVER crash when attempting to log these attributes through SpectroWATCH. Any customer created SpectroWATCHes, GIB views, or other customizations or extensions involving the old attributes must be changed to use the new attribute IDs. Here is the complete list of old/new attribute IDs.

Attribute Name	**Old ID**	**New ID**
actSrc	0x210120	0x211252
actDst	0x210121	0x211253
ckactSrc	0x210127	0x211254
ckactDst	0x210128	0x211255
locIPHelper	0x210112	0x211256
locIPWho	0x210111	0x211257
locRtMask	0x210118	0x211258

SPECTRUM 6.6 Feature List

This section describes new features included in SPECTRUM Version 6.6. Additional enhancements are included in this Service Pack 5 CD release. Those additional enhancements are discussed in the respective Software Release Notes for the Web downloadable versions of 6.6 Service Packs 1, 2, 3, 4, and 5, which can be accessed at: http://www.aprisma.com/support/secure/download/index.cgi?rev=06.06.00

AutoDiscovery

One of the many goals for SPECTRUM 6.6 was to improve AutoDiscovery in the areas of performance, accuracy, and overall usability. Below is a list of all the significant changes that have been made and a brief description of their impact.

Performance

- *Enhanced error checking:* Often device firmware errors cause blank lines to appear in some SNMP tables. Code has been inserted into AutoDiscovery to handle these anomalies.
- *Router Discovery Enhancements:* The IP router discovery algorithm has been rewritten to improve table read efficiencies. This new functionality should be most noticeable on routers with large SNMP tables. These increased efficiencies will also decrease the load associated with SNMP discovery on the router.
- *Enhanced use of proprietary discovery protocols*: Several enhancements were made to AutoDiscovery to ensure complete usage of proprietary discovery protocols (CDP, EDP, SDP).
- *Model Activation*: Changes were made to decrease model activation time at discovery or server restart.
- *Lightweight VLAN model*: Changes were made to the VLAN port model type to make it more efficient and decrease the amount of system resources it requires. The end result is faster model activation time and better overall SPECTRUM performance.

- *Reduction in Model Count and Memory Usage*: Model count and memory usage were reduced by no longer automatically discovering/ modeling unnecessary EthernetIfApp application models. These may still be generated, if needed, by initiating a manual application rediscovery from a device's configuration view.

Accuracy

- *Fanout models*: Additional intelligence has been added to review fanout placement. Previous releases of SPECTRUM would place a fanout between devices when the connecting device was unmanaged. When the connecting device was subsequently managed, the fanout would remain. The new intelligence will look for this condition and remove the fanout.
- *Multi-link Technology*: Enhancements were made to ensure more accurate device connectivity for multi-link technologies (Smarttrunk, Etherchannel, 802.3AD).
- *Spanning tree*: Enhancements were made to the spanning tree discovery algorithms to ensure more accurate connectivity mapping.
- *End station mapping*: Additional intelligence was added to assist in mapping end station connectivity.
- *Layer 3 Discovery*: Changes were made to the layer 3 discovery options to eliminate any layer two discovery dependencies.

Smart Defaults

- *Auto placement*: Changes have been made to the auto place models functionality to make the results more usable. A common task associated with the old auto place functionality was to edit the results to move the models closer together for better screen usage. New with 6.6, the auto place option will place models closer together to ensure better use of screen real estate. The default setting in the AutoDiscovery GUI will remain none, but if the user selects radial, their results will be closer together.
- *Zoom-to-fit*: Enhancements have been made to the zoom-to-fit feature to ensure complete screen usage regardless of screen resizing.
- *ATM Discovery*: An additional setting will be presented to the user to allow them to enable ATM discovery. By default, ATM discovery will be disabled.

- *Universe settings*: Changes have been made to the default universe settings to provide a cleaner modeling presentation. New Defaults: 1) Create routers in this view only 2) Place LANs in this view only 3) Create LANs.
- *Loopback and Duplicate IP support:* A change was made in SPECTRUM to allow models to exist that have duplicate IP addresses. Some networking technologies such as load balancers create identical IP addresses across a range of devices. Also, users occasionally configure the same loopback IP address across devices in order to simplify connections for local management. SPECTRUM AutoDiscovery will now be able to discover and model these unique environments.
- *Live Pipes*: The live pipes configuration intelligence was improved to persist the port polling status even if the connection off that port is removed and a new connection is modeled. Therefore, if the previous connection to the port had a live pipe, future connections to that port model will be live.

General Usability

- Modeling capabilities for Catalyst boards have been enhanced to allow the modeling of multiple boards with the same serial number.
- AutoDiscovery will now perform a layer-three mapping of existing device models as well as those that are being newly added by the AutoDiscovery application.
- Users will now be able to open and delete multiple AutoDiscovery result sets at once by using their mouse in conjunction with either the "Control" or "Shift" keyboard buttons.
- Container-based AutoDiscovery can now populate containers of customer-created model types derived from Network, LAN, and other key container model types.
- All modeling information that is displayed during the AutoDiscovery process will now be logged in the AutoDiscovery logs directory.
- Users will now have the ability to get an event after a router reconfiguration event completes. This is helpful in initiating post-reconfiguration scripts for model updating. In addition, if scripting is used to reconfigure like models in a large environment, this provides the user with visibility into which models failed to be reconfigured.

- Database check and backup will now occur prior to completing AutoDiscovery. The check provides the user with a warning if their database is corrupt prior to starting AutoDiscovery and allows them to restore a non-corrupt database. The backup then ensures they have a clean backup available moving forward if there is a problem that occurs during the discovery.

Distributed Install

- Users will now be able to complete distributed, multi-platform remote installations of all core SPECTRUM components and patches via command-line configuration files and utilities from a single host system.

Event and Alarm Management

- AlarmNotifier was enhanced to provide flexibility in determining the events to be viewed for each alarm. Users can now choose to show all events or view a summary of events where duplicates have been removed.
- Error checking and messaging in AlarmNotifier was enhanced to provide better, more meaningful error messages when errors occur within EventFormat files.
- Read-only users are now able to acknowledge alarms if the "Alarm Update by Read Only" attribute is set to true on the AlarmMgmt model.
- When retrieving alarms using AlarmNotifier, if a DLCI ports goes down, the IP address for the logical DLCI port will now be displayed instead of the primary IP address of the device.
- The Clear User Preferences menu pick will now be disabled for Read-Only users.

Maintenance Mode

- Users can now enable maintenance mode for individual interfaces/ports of a device. Interfaces/ports in maintenance mode behave in the same manner as devices in maintenance mode. No alarms or events will be asserted on the interface/port while in maintenance mode. SPECTRUM will send no SNMP or ICMP communications to the interface/ports while

in maintenance mode. Additionally, loss of contact alarms will be suppressed for devices, WA_Links, or fanouts connected to a port in maintenance mode. If a link down trap comes in for a port in maintenance mode, no alarm will be asserted on the device or the port model.

- Predefined searches have been added to the SPECTRUM Search Manager to allow users to rapidly find all interfaces/ports currently in maintenance mode.
- The image/icon presented when a dialup link is in maintenance mode has been refined to more clearly show that its status is maintenance rather than in use.
- The WA_Link display has been enhanced so that the color displayed is brown if the WA_Link is placed in maintenance mode. The color is green if a device attached to the WA_Link is placed in maintenance mode.
- When a device is placed in Maintenance Mode, the pipes associated with the device will now go brown as well.
- If SPECTRUM loses contact with devices downstream from a port or device in maintenance mode, the lost models will now be reflected in the Impact Severity and Impact Scope of the maintenance mode alarm. Therefore, when a device or port is put in maintenance mode, a brown alarm is immediately created for that model. The Impact Severity of that alarm will be zero. If the server later loses contact with the two devices downstream from the brown device or port, the two device models will go gray. In addition, the Device Criticality of those two device models will be added to the Impact Severity of the brown (maintenance alarm), and the Impact Scope view of the brown alarm will show the two lost device models. When SPECTRUM regains contact with the downstream devices, they will be removed from the alarm impact.

MPLS Manager

- MPLS Manager provides an extension to the current SPECTRUM Service Assurance modeling architecture. SPECTRUM modeling has been extended to introduce the concept of modeling the logical layer connectivity within an MPLS enabled infrastructure. As a result, two new modeling paradigms have been introduced. The first is the paradigm of a “path” model, which models an individual, end-to-end

connection through an MPLS enabled infrastructure. A Path model will provide a logical representation of many physical elements, such as devices, interfaces and links. The second modeling paradigm is the "LSP" model, which represents the logical data path through the MPLS infrastructure. An LSP model will consist of the primary and N secondary paths required to traverse the MPLS infrastructure. SPECTRUM MPLS Manager will discover these logical layer models when discovering and modeling the physical devices.

Mulitcast Manager

- SPECTRUM's Multicast Manager is designed to provide management for multicast traffic within your network environment. This includes the identification and monitoring of all multicast groups, sources, receivers and other critical resources like rendezvous point routers. Multicast Manager discovers and models Cisco devices that support multicast. Once these devices have been discovered, Multicast Manager provides several views which allow you to monitor the connectivity of these multicast elements. These views offer details relating to multicast groups, sources, receivers, routers, and rendezvous points and their relationships to each other. The information provided in these views makes troubleshooting multicast related outages much more efficient. You can pinpoint a problem quickly because you can determine the group a receiver belongs to, the rendezvous point of the group, the source for the group, the routers and interfaces a group uses, and the configuration and bandwidth limits of these interfaces. Based on this information, you can prioritize your troubleshooting efforts should multiple problems occur. Multicast Manager is accessed through the SPECTRUM Web Operator interface.

New Management Modules

- *Cisco 4500 Series MM:* SPECTRUM management module SM-CAT1010 currently provides modeling for the following Cisco Catalyst 4500 Series devices*:*

Device	Firmware	Model Type
Catalyst 4507R (7-slot: redundant Supervisor IV capable)	Cisco IOS 12.1(13)	SwCat45xx
Catalyst 4506 (6-slot)		
Catalyst 4503(3-slot)		

- *3Com 4400/4900 SuperStack Switches MM:* SPECTRUM management modules SM-3CM1012 and SM-3CM1013 currently provide modeling for the 3Com devices:

Device	Firmware Revision	Model Type
4400 (3C17203)24 Port SuperStack III Switch4400 (3C17204)48 Port SuperStack III Switch4400SE (3C17206)24 Port SuperStack III Switch	v1.0, v2.0,v3.0	3Com44xx
4900 (3C17700) 12 Port SuperStack III Switch 4900 (3C17701) 24 Port SuperStack III Switch 4900SX (3C17702) SuperStack III Switch 4095 (3C17706) SuperStack III Switch 4050 (3C17708) SuperStack III Switch 4060 (3C17709) SuperStack III Switch	v1.0, v2.0, v3.0	3Com49xx 3Com40x0

- *Enterasys Matrix E1 Series MM:* SPECTRUM management module SM-ENT1007 currently provides modeling for the Enterasys Matrix E1 Series devices:

Device	Firmware	Model Type
1H582-51 Workgroup Switch (WS)	Standard: 2.04.12 Federal: 2.04.10	MatrixE1
1G582-09 Gigabit Workgroup Switch (GWS)	2.04.12	
1G694-13 Optical Access Switch (OAS)	1.02.04	
1H582-25	2.04.12	

- *Arris Cadant C4 CMTS MM:* SPECTRUM management module SM-CIS1020 currently provides modeling for the following Arris Cadant C4 CMTS devices:

Device	Firmware Revision	Model Type
Cadant C4 Cable Modem Termination System	Firmware 3.0.2	CadentC4
	Firmware 3.0.3	
	Firmware 3.1.1	
	Firmware 3.2	

- *Cerent 15454 Optical Router (Cisco ONS 15454) MM:* SPECTRUM management module SM-CIS1020 currently provides modeling for the following Cisco ONS 15454 (formerly Cerent) devices:

Device	Firmware Revision	Model Type
Cisco ONS 15454 SONET Multiservice Provisioning Platform (MSPP)	03.20-002C-19.20	CerentONS15000

- *Enterasys X-Pedition Security Routers MM:* SPECTRUM management module SM-ENT1006 currently provides modeling for the following Enterasys X-Pedition Security Routers:

Device	Firmware Revision	Model Type
XSR-1805	XSR-1800 Series, Release 4.0	XPedSecRtr
XSR-1850		

- *Sun Fire B1600 MM:* SPECTRUM management module SM-SUN1001 currently provides modeling for Sun Fire Blade Platform devices such as the Sun Fire B1600 Intelligent Shelf:

Device	Firmware Revision	Model Type
Sun Fire B1600	pre-released	SunFireSw

- *Nortel Contivity MM:* SPECTRUM management module SM-NTL1004 currently provides support for Nortel's Contivity family of VPN switches and provides IP Fault Management visibility:

Device	Firmware Revision	Model Type
Contivity 100	Instant Internet 7.11 and 7.2	ContivityVPNII
Contivity 200		
Contivity 400		

Device	Firmware Revision	Model Type
Contivity 600	Contivity Extranet Switch 4.05, 4.06, and 4.5	ContivityVPN
Contivity 1000		
Contivity 1010		
Contivity 1050		
Contivity 1100		
Contivity 1500		
Contivity 1600		
Contivity 1700		
Contivity 2000		
Contivity 2500		
Contivity 2600		
Contivity 2700		
Contivity 4000		
Contivity 4600		

- *Cisco 3000 Series MM:* SPECTRUM management module SM-CIS1017 provides support for Cisco's 3000 family of VPN switches and provides IP Fault Management visibility:

Device	Firmware Revision	Model Type
Cisco VPN Client 3002	3.5	Cisco3xxxVPN
Cisco VPN Client 3005		
Cisco VPN Client 3015		
Cisco VPN Client 3030		
Cisco VPN Client 3030		
Cisco VPN Client 3060		
Cisco VPN Client 3080		

- *Cisco CallManager MM:* SPECTRUM management module SM-CIS1019 provides support for Cisco's CallManager. The MM provides support for the Cisco CallManager (CCM) MIB. Supported MIB groups include the

"ccmTable" (CallManager) MIB group, "ccmGatewayTable" group and the "ccmGatewayTrunkTable" group. These tables provide the user insight into the health of the CallManager as well as information on the gateway connected to the CallManager. CallManager specific traps will be supported and will be available to the user as SPECTRUM event and alarms. Lastly, this management module will support the integration of the web-based CCM Administration suite.

- *Enterasys RoamAbout 2 MM:* SPECTRUM management module SM-ENT1002 provides support for Enterasys' RoamAbout R2 family Wireless Access Platform LAN switch and provides IP Fault Management visibility:

Device	Firmware Revision	Model Type
RoamAbout R2 Access Point	2.00.16	RoamAboutR2

Enhanced Management Modules

The following IETF RFCs are now supported in this release

- *RFC1724 (RIPv2):* This RFC provides information relating to the RIP2 standard routing protocol. It includes the following views:
  - "Global Counters" – which shows the number of route changes and queries
  - "IF Status" – RIP statistics per interface
  - "IF Configuration" – RIP2 configuration setting per interface
  - "Peer Table" – provides information about active peer relationships intended to assist in debugging.
- *RFC2737 (Entity MIB):* This RFC provides information relating to components of a device (i.e. physical interfaces, boards, fans, etc.). SPECTRUM uses this information to provide physical and logical component descriptions, their respective relationships, and their statuses. Additionally, trap support that notifies SPECTRUM of the device's physical and logical component changes has been added.
- *RFC2618 (Radius Authentication Client) and RFC2620 (Radius Account Client):* These RFCs expose information relating to centralized user password authentication services and the centralized user password account information for the authentication services which are frequently deployed in various VPN and Wireless networks.

- *RFC2667 (IP Tunnel MIB):* This RFC provides information pertaining to tunnel protocols that are established over IP. It also provides the public IPs that a tunnel is established over.

In addition, several other enhancements were made to existing management modules.

- The Nortel Passport MM was enhanced to ensure SNMP requests are properly received thereby enabling SPECTRUM to properly resolve the devices connections completely.
- The Compaq Insight Manager Management Module has been enhanced to support the Compaq Threshold MIB. All objects defined in this MIB are available from the Host Compaq model type. Additionally, two new views were added: Threshold Alarms Information and Threshold Agent Information. The Threshold Alarms Information view provides insight into Compaq's threshold management, including Poll Frequency as well as an Alarm Table containing extensive alarm detail. The Threshold Agent Information view provides insight into agent polling settings, major and minor MIB revision settings, and an Agent Table populated with Name, Version Date, and Purpose.
- The Cisco IGX management module has been updated to include comprehensive physical interface modeling and integration with ATM Circuit Manager as well as Frame Relay Manager.
- SPECTRUM Configuration Manager now supports the following Cisco device models:
  - Cisco6400_DSL
  - HubCat29xx
  - SwCat85xx
  - SwCat35xx
  - SwCat45xx
- The Alteon Acedirector was updated to include support for firmware 10.0.26 and AceDirector4.
- Cisco Aironet was updated to include support for Cisco 1200 AP and the following new mib: AWL-VLAN-CFG-MIB.
- The Brocade management module has been updated to include support for the 3000 and 12000 device families. MIB access support was also enhanced to include the Fibre Channel Management Framework Integration MIB (FCMGMT_MIB), versions 3.0 and 4.0 of the Fabric

Element MIB (FCFABRIC-ELEMENT- MIB), and version 4.0 of the Enterprise Switch MIB (SW- MIB). Five new traps, introduced with FCMGMT_MIB, are now mapped.

- The Motorola Vanguard management module has been updated to include management of the Vanguard 6435 and 6455 devices. Additional enhancements include: comprehensive physical interface modeling; full trap support; and Frame Relay Manager integration.

Non-Persistent Connection Manager (NPC)

- Support for Multilink PPP has been added by allowing a Dialup_Link model to be pasted on more than one interface on a single device model. When the Dialup_Link model is pasted on each of the PPP interfaces which make up the multilink, these interfaces will form a secondary group. A new Dialup_Link model attribute, DevSecGrpActiveCriteria, controls the method used to determine the state of a secondary group, and thus the secondary link. This attribute can be set from the Dialup_Link 'Information' GIB view to the following values: “Any Secondary IF Active” - If any member of the secondary group is active, then the multilink is active; “All Secondary IFs Active” - If all members of the secondary group are active, then the multilink is active.
- Support for Dialer Profile configurations has been added by allowing Dialup_Link models to be pasted on the Dialer interfaces. These logical interfaces represent a call to or from a particular peer. At call time, a Dialer interface will dynamically bind to a physical interface which is selected from a Dialer pool. Specialized intelligence was implemented to infer the operational state of Dialer interfaces from its ifAdmin/ifOper values as well as the state of any physical interfaces it may be bound to.

Process Daemon

- Processed now runs as a Windows service, which lets SPECTRUM continue to run on a Windows machine even if the Windows user logs off the machine. When installing SPECTRUM in the Windows environment, you will be prompted to enter a username and password in the Windows Service Configuration dialog box. This username and password can be either a local machine account or a domain account

and will be the account that the processd service uses to start server processes that must stay running when no user is logged in.

- There are now two main differences in the operation of processd in the Solaris and Windows environments due to differences in their native security architectures:
  - When you request the start of any process (such as the SpectroSERVER or the Archive Manager) from a remote connection in the Windows environment (typically using the SPECTRUM Control Panel), the process will always start as the processd server user. In the Solaris environment, the process will start as the user making the request.
  - For server processes that need to stay running after a user logs out, a new SERVERPROCESS field was introduced for the Windows environment. In order for Windows to not shutdown these processes during logout, these server processes are started as the user configured to run the processd service (not the TICKETUSER specified in the install ticket in the Solaris environment).

Service Performance Manager (SPM)

- Service Performance Manager (SPM) is an application designed to allow you to configure and view results of Response Time Test measurement across Distributed SpectroSERVER domains and throughout the managed network. SPM offers a multi-vendor, multi-agent approach to response time management, enabling existing performance management investments to be leveraged. Intelligent, automated discovery and configuration of performance test points within the infrastructure accelerates deployment and optimizes workflow efficiency. The user interface to the Service Performance Manager is entirely web-based and supports the Network Operations Center (NOC) workflow processes.

SPECTRUM Reporting Gateway

- With the SPECTRUM Report Gateway (SRG), Aprisma has provided a gateway to convert and archive raw SSLogger data into Round Robin Databases (RRD). Once SSLogger data is in RRD format, there are many different tools and utilities available to generate graphical reports. The SRG utilizes SSLogger as its data-collection engine, RRDtool as a means of efficient SpectroSERVER data storage (RRD

creation), and Cacti or DDRAW to graph the resulting data sets. Note: RRDtool, Cacti, and DRRAW are open-source applications (available under the terms of the GNU General Public License) used with the SPECTRUM Report Gateway. These and other referenced open-source products are not designed, developed, or supported by Aprisma Management Technologies.

SNMPv3

- The ability for users to manage SNMPv3 devices with SPECTRUM, including SNMPv3 GET and SET requests, and Traps and Informs, is now available. Users will have the full range of SNMPv3's authentication and encryption capabilities available to support fully secured management traffic. A new "Model-by-IP" dialog allows the user to select whether a new device should be managed through SNMPv3, and if so, provides the user with options to choose the authentication/ encryption level and provide the relevant security parameters. Note that SPECTRUM AutoDiscovery does not support automated discovery and modeling of SNMPv3 devices.

SPECTRUM Configuration Manager

- SPECTRUM Configuration Manager "save as" capabilities have been enhanced to allow the current configuration to be written to a file with the name devicename_config name.txt. This translates to easier archival of configurations.
- The risk of a customer router staying in an infinite "wait" state and SPECTRUM Configuration Manager hanging has been removed. By leveraging a timer to give the device time to respond, reducing the server load, and adding a counter for "wait" messages, the load will automatically be stopped when necessary and the error "Router did not initiate tftp transfer in time" will be presented to the user.
- The performance of SPECTRUM Configuration Manager has been enhanced when displaying large amounts of data from Host Configs comparisons.

Trap Handling

- For unmanaged and unmapped traps, the user will now have access to all trap information. When a trap is received by SPECTRUM for which

there is no trap mapping or the element is not modeled in the SPECTRUM object database, all varbind data will be captured and presented to the user in a SPECTRUM event associated with the trap.

- Customers who add SNMP trap mappings through AlertMaps can use a new global scope alert mapping by creating a new subdirectory in the CsVendor area and placing an AlertMap file there. Previously, AlertMap trap mapping entries were required for every model type that needed to support the trap. Now only one "global scope" AlertMap entry is required for a trap to be supported/mapped across all modeled devices. These files will be preserved on upgrades.
- The trap mapping functionality is no longer available in the Event Configuration Editor. However, it is still possible to map traps by directly editing the appropriate AlertMap file. Instructions for doing this can be found in the *Event Configuration Files Guide (5070).*

Web Operator Suite

- The amount of unused screen real estate and secondary graphics and logos has been reduced to increase the amount of useful data that can be presented on a screen. This reduces the amount of scrolling and the need for the user to "hunt" for data.
- The Web Operator Suite home page has been removed and users will now be initially presented with the Alarm Manager after logging into the product.
- Alarm Manager no longer refreshes automatically by default. Users can choose when to refresh or they can activate the automatic refresh.
- Alarm severity is now indicated in the alarm table by the background color of the alarm's table row. Critical alarms are red, major alarms are orange, and minor alarms are yellow.
- When using the filter in Web Alarm Manager on a larger number of alarms (>3000), filtered alarms will now be displayed at the top of the list just as they are in Spectrum Alarm Manager.
- The Alarm Manager's alarm table now includes a single details column that presents the user with all of the needed "click areas". From here users can choose to click to the alarm details, model information, alarm type information, as well as the secondary alarms.

- Alarm Impact Severity has been added to the main alarm table, and the Impact Scope View, formerly only available in the desktop Alarm Manager, is now available by clicking on the Impact Severity column.
- Alarm type data, including alarm name, probable cause, symptoms and recommendations, is now presented on the alarm details page. Users will no longer need to drill into another Web Operator Suite screen.
- User administration has been removed from the Web Operator and is now part of the standard Spectrum User Editor - Spectrum user administration no longer takes place from multiple areas of the system.
- Checking and messaging during install has been modified to ensure the user is notified if they try to install Web Operator to a directory with a space in the name. They will be prompted to select a different directory if they try to do this.
- Page context-sensitive launch capabilities have been added to allow users to launch into a web-based, searchable version of the *SPECTRUM Web Operator User Guide (5078)*.
- If BMC PatrolView Integration is in place, visibility of parameters below applications has been enhanced by creating another link below the Application Class that displays a view for all the parameters of each class.

VPN Manager

- The VPN Manager is an application that is designed to allow you to discover, model, and monitor VPNs within the network environment. VPN Manager provides VPN and Site discovery and modeling, VPN connectivity status, SNMP trap handling, monitoring of Virtual Routing and Forwarding (VRF) condition, and performs calculation of and alarming on VPN condition. VPN Manager is accessed through the SPECTRUM One Click interface.
- The VPN Manager currently supports the IETF draft MPLS/BGP VPN MIB (draft-ietf-ppvpn-mpls-vpn-mib-05) and Cisco's MPLS Virtual Private Networks MIB (MPLS-VPN-MIB). These MIBs provide access to configuration information for VPNs configured on Provider Edge Router (PE) interfaces. This information lets VPN Manager discover all of the PE routers and interfaces that are forwarding traffic for a particular VPN. Based on this discovery, SPECTRUM will create VPN models representing each unique VPN. These VPN models can then be polled for their current operational status (Up or Down).

- VPN Manager provides searches that let you quickly find a particular VPN or conduct a search for all VPNs. Search results contain a list of the current VPNs configured within the environment and the current status. You can drill into a single VPN to see the current list of PE interfaces participating within that VPN as well as the VPN's current status.

Performance

- Watch Editor performance has been increased by only displaying a subset of affected models, therefore minimizing the time users wait to retrieve their requested list of models. The number of models to display at any given time will be user-definable. The user will be able to "page" to the remaining undisplayed models at their convenience.
- Search Manager Performance for large searches has been enhanced by refining underlying search infrastructure.
- The amount of traffic generated by WA_Link models has been decreased to decrease SpectroServer CPU utilization.
- Adjustments have been made to increase performance while using "use the same View" preference with a large number of pipes in the view.

Additional Usability Enhancements

- For Frame Relay management, users are now able to view IfIndex, IfDescription and IP address within the DLCI_Port Configuration GIB view.
- Column headers in Global Attribute Editor were updated to better describe the purpose of the data that falls in the "default" column.
- Results provided from "Ping through Server" are now provided using the IP address argument instead of the model name, thus providing cleaner/clearer output.
- Usability of "Ping through Server" has been enhanced by implementing shorter time outs and providing "Request timed out" messages to end user.
- The VLAN List menu pick is now enabled and selectable in the Universe View when the user has a device modeled in the Universe View that has VLANs configured.

- The “Bring to Front” and “Send to Back” changes made via the Edit mode in the SpectroGRAPH are now saved to the GIB for the current view so that a restart of the SpectroGRAPH displays the desired change.
- Automatic map entry timeouts have been added to allow distributed SPECTRUM component entries to age out. This benefits the performance and usability of the server selection start-up dialog of the Control Panel and other distributed applications. This also eliminates manual map update steps that were previously required to eliminate defunct map entries as customer’s distributed SPECTRUM deployments changed over time.
- SPECTRUM Southbound Gateway EventAdmin models may now be placed into Container models to alleviate clutter in the Universe view.
- Event Configuration Editor now supports configuring the clearing of multiple alarms with a single event code.
- MIB2 Link UP/DOWN traps will now trigger an update to link status associated with WA_Link models only so that the user doesn't have to wait for an alarm to know that something has happened.

Miscellaneous Enhancements

- Multiple telnet sessions can now be run at any one time.
- Management Neighbors and live pipes is now documented in the *How to Manage Your Network with Spectrum Guide (1909)* to better support users ability to set this up correctly and get expected and useful results.
- Modeling Gateway can now be used to destroy models that have been completely removed from the network.
- The data type of the data_relay_port model type’s ifDescr attribute was changed from Octet String to Text String to allow that attribute value to be human readable when queried through CLI. Also, the MTE was modified to allow for existing attributes to have their data type changed from Octet String to Text String. A utility script was added to the product distribution (in the vnmsh/sample_scripts directory) to allow customers to convert Octet String attribute values returned by CLI to readable text.

Corrected Issues

This section describes issues that have been corrected in SPECTRUM 6.6. Additional corrected issues are included in this Service Pack 5 CD release. Those additional corrected issues are discussed in the respective Software Release Notes for the Web downloadable versions of 6.6 Service Packs 1, 2, 3, 4, and 5, which can be accessed at: http://www.aprisma.com/support/secure/download/index.cgi?rev=06.06.00

ATM Manager

Corrected Issues: ATM Manager

Item	Problem	Resolution
1	The ATM Circuit Manager Logical Connection View was not reporting the correct status of modeled ATM circuits if the view was left open. The view was polling load values but only determining the link condition when the view was opened.	This was resolved by polling the link condition attribute and updating the link condition column in the LCView if the status changed. This fix ensures that the correct status will display if a link condition changes while the Logical Connection View is open.

AutoDiscovery & Modeling

Corrected Issues: AutoDiscovery & Modeling

Item	Problem	Resolution
1	When an Adtran device was discovered, it was not resolving to the correct interface of the host device.	This was resolved by ensuring AutoDiscovery correctly maps devices with a `DataRelayClass` of "0". The attribute, `isEndStation/0x1296b`, was obsoleted from the core database.

Corrected Issues: AutoDiscovery & Modeling

Item	Problem	Resolution
2	When completing an AutoDiscovery of 2700 routers (that were already active), AutoDiscovery hung for a few hours after printing the following message in the AutoDiscovery GUI: "Model creation finished: created 1 model". Java exceptions were causing the GUI to hang.	This was resolved by presenting the errors to the user to ensure he/she knows the exception has happened and can then make the choice to either continue or exit.
3	When changing a Cabletron device model's community string via Search Manager, the model information view did not always populate the change down to the port and application child models of the device.	This was resolved by adding `COMMUNITY_STRING` to the list of attributes to roll down to port models for Cabletron 6xxx_xx, 9xxx_xx, and 2xxx_xx model types. The Cabletron 6000 series model type was also updated to allow the community string to be rolled down to application models.

CLI

Corrected Issues: CLI

Item	Problem	Resolution
1	The user was trying to do an update on action `2162696`, and they got a message after completion, "update: Failed." Looking at the action, it completed successfully, but reported incorrectly that it failed. This occurred because SPECTRUM was sending Cabletron specific action to all devices when application rediscovery was invoked.	This was resolved by no longer sending the Cabletron specific action during application rediscovery.
2	When trying to update the `ip_address` attribute (`0xc40253`) or (`0x10e43`) with a value of `0.0.0.0` using CLI (update), the update command failed with the following error message "update: 0.0.0.0: invalid value". Using the SpectroGRAPH, however, the user was able to update the DLCI port ip address without any errors.	This was resolved by adjusting the code to allow CLI to update attributes with `0.0.0.0`.

Database, Data Export, & Reports

Corrected Issues: Database, Data Export, & Reports

Item	Problem	Resolution
1	Reports: When a scheduled entry was saved and the Scheduler dialog was closed, the saved scheduled entry did not get listed when the Scheduler dialog was reopened.	This was resolved by making adjustments to show the scheduled entry when the Scheduler dialog was reopened.
2	Reports: When launching Spectrum Report Generator (SRG) from an Organization Chart after selecting approximately 200 models, the report generator crashed at runtime. This was caused by a memory allocation problem when using NT.	This was resolved by inserting code that dynamically allocates memory.
3	Reports: Performance was severely degraded when running reports with >50,000 models of same type. This was caused by the user opening the SRG and clicking the Models button before the necessary queries were run.	This was resolved by adding a watch cursor while the UI is waiting for a response. Now, the user knows that processing is occurring and will not inadvertently cancel the necessary queries.

Event & Alarm Management

Corrected Issues: Event & Alarm Management

Item	Problem	Resolution
1	Alarm Manager: The user was seeing a memory leak when running their CORBA application in 6.5.0.	This was resolved by adjusting the code to remove the leak.
2	Alarm Manager: Read-only users (ADMIN, 5-9 or anything, 5-9) did not have access to the information or buttons in the Location Tab within any of the PGUI applications. This was only found to be the case for port models and only found to be a problem with 6.5.0 and 6.5.1. If a ReadWrite user accessed the Location Tab for the same model in any of the PGUI apps (Alarm Manager, Search Manager, Event Manager), there was no problem. The ReadWrite user could not only see the Location Tab information, they could also use the button to navigate to the model.	This was resolved by adjusting the registry for ID_TOP_MH (CsIHTechSubIntBase) to only require read only privileges.
3	AlarmNotifier: The order in which the notification data was given to AlarmNotifier was following reverse order.	This was resolved by changing the order in which the notification data is given.
4	AlarmNotifier: AlarmNotifier didn't update when a new event was added to an existing alarm.	This was resolved by modifying the event field of the alarm stored in SANM upon an event change.
5	AlarmNotifier: The `AlarmNotifier` resource `STREAM_EVENT_MWSSAGE` was not working if placed at the end of the `.alarmrc` file.	This was resolved by adjusting the code to function regardless of where the message is located within the file.
6	AlarmNotifier: AlarmNotifier was experiencing performance issues and not processing new alarms after adding new landscapes to a policy. When invoking a SSAPI request to get an Alarm Management model, the pending SpectroSERVER requests were increased but never decreased when a notification was received.	This was resolved by adjusting the code to correctly decrement the pending SpectroSERVER requests for a SSAPI request to get an Alarm Management Model.

Corrected Issues: Event & Alarm Management

Item	Problem	Resolution
7	EMS: The event format file for event 210010 enumerated the 3rd variable of the event in a table. It should have been the second variable that was enumerated. There is no third varbind sent in the trap.	This was resolved by adjusting the file to show the correct information in the appropriate place and format.
8	Event Manager & Alarm Manager: The user received an error obtaining the current time from VNM when logging in as a non-Admin user.	This was resolved by creating a new required model type that contains non secure read only attributes, such as current time. The new model type does not have a security string set so it is accessible by anyone.

Fault Tolerance

Corrected Issues: Fault Tolerance

Item	Problem	Resolution
1	Old alarms appeared to "regenerate" on the primary SpectroSERVER when a database synchronization was done to the fault tolerant secondary SpectroSERVER. It appeared that the secondary SpectroSERVER was regenerating these alarms when it came back up, and was logging the events to the Archive Manager running on the primary SpectroSERVER system. This was being caused by the 3 - 4 minute lag of the switch-over from primary to secondary on the restart of the secondary after a db sync.	This was resolved by having the system read the primary SpectroSERVER's `VNM_UP_TIME` attribute following a failure. It will now switch over immediately if this is greater than or equal to three minutes.
2	A user model information error message was being received by the SpectroGRAPH during a failover from the primary to the secondary SpectroSERVER. This was caused when an attribute watch registration failed because the secondary SpectroSERVER had not yet detected that the primary SpectroSERVER was down.	This was resolved by having the secondary SpectroSERVER attempt to poll the primary SpectroSERVER when a client request fails. If it cannot contact the primary it will switch to primary mode and re-dispatch the request to its local landscape.

Installation

Corrected Issues: Installation

Item	Problem	Resolution
1	Installation crashed when the Install User Name exceeded the limit (20 characters for a username on NT, not including the domain and 64 characters for Solaris).	This was resolved by increasing the maximum length allowed for User Name.
2	Patches were intermittently failing when unzipping vtapes.	This was resolved by replacing `gzip | newtar` with a version of newtar that handles gzip compression internally.

Location Server

Corrected Issues: Location Server

Item	Problem	Resolution
1	User's `.hostrc` files contained only + and the server `.hostrc` had host names that could not be resolved by dns. When reading the `.hostrc` file, each entry was validated (that is, tested to be sure that the machine exists) by SPECTRUM. In the case of machines which were either down or non-existent, the validation timed out. When there were a number of non-existent machines, this timeout was repeated for each one. These timeouts could add up to a significant delay in starting applications which use the `.hostrc` file.	This was resolved by ensuring that `processd` checks to see if the `.hostrc` file has been changed (by using `stat()`) before re-reading it.

Miscellaneous

Corrected Issues: Miscellaneous

Item	Problem	Resolution
1	Live Pipes: When the port models in the port link list node were zero, the user received "Access Denied message" in Enable Live Pipe GIB View.	This was resolved by adjusting the code to skip permission checking on the model if the model handle is zero.
2	Online Backup: A user attempted to perform online backups on his Windows machine but the backup failed because the `tmpdir` directory was not being removed. After troubleshooting the issue, it was found that the location of the `Backup Directory` did not include the Windows drive letter.	This was resolved by modifying the code so that when SS creates the backup directory specified by the user, it must check, when it runs in windows platform, if the drive exists in the backup directory or not. If it does not, it will update the directory with the current drive used.
3	`Processd` was crashing when there was a zero length runtime file in the runtime directory. It could occur the first time processd was started and stopped before the runtime file ever got written to disk.	To avoid `processd` crashing when reading in a zero length file, a change was made to first check the length of the file before reading it into memory. If the file is zero length, it is removed.

Management Modules

Corrected Issues: Management Modules

Item	Problem	Resolution
1	ADC Cuda: The ADC_Cuda is a Chassis based device. Each card in the Chassis has its own CPU and thus its own discreet `SystemUpTime`. The system was displaying the Chassis `SystemUpTime` for the boards rather than the correct board `SystemUpTime`.	This was resolved by importing the mib that supports `basSysUpTime` into a model type `adc_alias_mib` that is derived off of the ADC model type. This was added to the base model type of ADC_Cuda and the database to allow customers to create the view(s) they wish to implement using attributes from the database.
2	Spectrum was not able to detect variable varbinds associated with ADC Cuda traps. Extra spaces in the Event files and missing enumerations in the `EventTables` were causing the problems that were being seen.	This was resolved by adjusting the formatting in the Event files and adding entries for the new enumerations in the EventTables.
3	ATM Circuit Manager: `AlertMap` file name for `Nortel_PP/pp_3_slot` had a lower case "m" in `AlertMap` rather than an upper case "M".	This was resolved by changing the "m" to "M".
4	Some ports were not displaying in the DevTop view of the HubBaySt450 model.	This was resolved by adjusting the code that determines duplicate board/port associations on the HubBaySt450. This prevents valid ports from being eliminated and not displayed in the DevTop view.
5	Cabletron: When a 2H252_25R with SecureFast loaded was modeled, it showed a switch sticky label in the center of the device icon on the topology view. When bringing up the DevTop view, the device icon showed a bridge sticky label. This also happened in the Device->Interface view. When bringing up the Application view there were no bridging application models shown. Instead there was an SFVlanApp.	This was resolved by modifying the file to correctly show a switch label rather than a bridge label.

Corrected Issues: Management Modules

Item	Problem	Resolution
6	A Cisco_Router management module was losing some links to DLCI_Ports when the model was reconfigured. This problem occurred after migrating from SPECTRUM 5.0rev1 and was caused by the Frame Relay `Internal_IF_Type` attribute being set to 0 instead of 32.	This was resolved by creating a new attribute that will check the value of an interface's `Internal_If_Type` upon SpectroSERVER startup and write the correct value if necessary. This check will only occur on the first startup after upgrade or install.
7	AutoDiscovery was not able to resolve connections to the upstream and down stream neighbors of Cisco devices that used CDP.	This was resolved by adding support to AutoDiscovery for reading CDP table connection information.
8	AutoDiscovery was not resolving some connections properly when the Layer 2 option, Source Address Table, was selected.	This was resolved by enhancing AutoDiscovery to include the default route when determining if a device is routing and removing the mutual hears requirement when creating a connection between ports.
9	Cisco Catalyst: The use of the variable `TIME` in both the `rcvBitsPerSecond` and `xmtBitsPerSecond` SpectroWATCH's was yielding inaccurate results and was inconsistent with the documentation.	This was resolved by modifying the default values for both the `SWD_rcvBitsPerSecond (0xc4063d)` and `SWD_xmtBitsPerSecond(0xc4063e)` attributes of the `CiscoAtmVclLnk (0x210074)` model type, so that the watch formula uses the `X_sysUpTime` variable instead of the `TIME` variable.
10	Cisco Catalyst: When modeling a Cisco Catalyst 3550 by IP, the device modeled as a Rtr_Cisco MT.	This was resolved by entering the SysOID of the device into the `SysOIDVerifyList` within MTE in order to recognize the device as a SwCat35xx MT.
11	Fault Isolation: Proper Management Neighbor modeling relies on which devices are upstream/downstream relative to the VNM. The Fault Isolation GIB, which explains Management Neighbor functionality, only tangentially touched on the concept of proximity to the VNM.	This was resolved by making the Fault Isolation GIB more descriptive.
12	Forerunner: SpectroWatch calculations for the attributes `SWD_rcvBitsPerSecond` and `SWD_xmtBitsPerSecond` were wrong.	This was resolved by changing the atmLinkDerPt model type so that all models deriving from it would inherit the fixed calculations.

Corrected Issues: Management Modules

Item	Problem	Resolution
13	Host Compaq: In 6.5, the cmpq app models were deprecated and the Host_Compaq model type inherited all the device specific attributes, and new GIB views were created. The user could not find views for the `cpqSePci` mib information that were there in 6.0.3. The attributes were there, but the user requested new GIB views.	Three new GIB views where created for `cpqSePciSlotTable`, `cpqSePciFunctTable` and `cpqSePciMemoryTable`.
14	Nortel Passport: Lack of error checking when models were created with the `Ntl_TrunkApp` caused the SpectroSERVER to crash. Specifically, this was caused by a lack of error checking in the `CsIHNPTrkMap.cc` IH.	This was resolved by inserting error checking on the strings prior to completing required manipulation.
15	The user discovered that on Wellfleet Router Models in the Application View, the GIB views off the wfIpApp were no longer populated with information. Specifically the Menu Picks for Gre Tunnel Information and Connections. The occurred because the attribute IDs listed in the corresponding Gib views were no longer part of the Application model. The Attribute IDs were changed but the Gib Views were not modified with this change.	This was resolved by modifying the Gib Views with the appropriate changes.

Dominion Web Reporter

Corrected Issues: Dominion Web Reporter

Item	Problem	Resolution
1	Archive Manager did not handle overflows well. Customers were seeing a MySQL generated error when SSAPI scroll requests contained a `count >= 2147483648`. The error message was similar to: "Native Error: 1064, You have an error in your SQL syntax near '4294967295' at line 1."	This was resolved by adding a check in the `CsLogManager::scroll_to` method to see if the scroll count is less than 2147483648. If the count is 2147483648 or greater, a Failure error is given and the offending request is printed out prior to returning.

Search Manager

Corrected Issues: Search Manager

Item	Problem	Resolution
1	While performing a custom search with Search Manager, the user found that "Polling Interval" was being displayed incorrectly.	This was resolved by modifying the calculations that are performed against Polling Intervals entered by the client before displaying the value.

Security

Corrected Issues: Security

Item	Problem	Resolution
1	After a SpectroSERVER restart, the second part of a security community string was being lost, and the security community string was being reset to that of the group in which the user belonged.	This was resolved by graying out attributes for User models for which the group model that they belong to has the common flag set. In addition, the SpectroSERVER will now return an error if someone tries to write to a User model attribute when the User belongs to a Group and the common flag is set on an attribute.

SpectroGraph

Corrected Issues: SpectroGRAPH

Item	Problem	Resolution
1	Within the application CsNewView, the `-ui` option was not working properly. Users expected that the new window to be opened would appear on the display of the value passed by `-ui`, but it did not.	This was resolved by changing CsNewView so that when no options are given, the `$DISPLAY` variable is used instead and allows the view to appear on a remote client.

Corrected Issues: SpectroGRAPH

Item	Problem	Resolution
2	More information was needed when a SpectroGRAPH received a "Permission Denied" error when it tried to connect to a SpectroSERVER. SecurityManager (SM) reads the `.hostrc` file after a SpectroSERVER is started or the `.hostrc` file is updated and tries to resolve all the host entries in `.hostrc` by OS Service. Sometimes the OS Service did not resolve the network address for some hostnames listed in `.hostrc`.	This was resolved by creating a new view to display unresolved host names. The VNM Control View -> Host Security Information view displays lists of resolved and unresolved hosts. Also, an event and alarm (Event00010e01, Prob00010e01) will be generated on the VNM when there are unresolved host names.
3	When the user, on NT 4.0, printed a SpectroGRAPH topological view, the sticky label icon was missing and not printed on the device model. It seemed that the problem was related to the GnSNMPDev model type. If the user modeled a device as a GnSNMPDev (or if it was derived from GnSNMPDev) and then selected "File"--"Print"--"Print View", the device was missing the sticky label icon of the triangle and the words "SNMP". The sticky label icon appeared fine in the GUI but was missing when the view was printed. This was also seen on Cisco devices; Cisco_2501/Cisco_2621, 4700, 4000, and Rtr_Cisco.	This was resolved by modifying the repaint method.
4	SpectroGRAPH was experiencing stability issues when a device DevTop view was opened that contained a Gen_IF_Port model that was displaying performance statistics.	This was resolved by adjusting the code that was not supporting 64-bit counters.
5	When running SpectroGRAPH on the Windows platform, links between certain models such a Rpt_Segment (Fanout) model and a Pingable model, will display green even though Live Pipes is not enabled on the link. Also, in these unusual cases, the link will stay green even when the modeled link is down.	This was corrected by making enhancements to Fault Management.

SpectroSERVER

Corrected Issues: SpectroSERVER

Item	Problem	Resolution
1	FlashGreenEnabled functionality was not working in 06.05.01.	This was resolved by adjusting the code so that when FlashGreenEnabled is set to "true" and a model's alarms are cleared, the model will flash green.

2	When available threads values were changed in the VNM -> Configuration -> Thread Information view GUI, the values were written to the database but the `$SPECROOT/SS/.vnmrc` file was not updated.	This was resolved by removing the default entries from the `.vnmrc` file to avoid confusion when the values are updated via the GUI.
		`max_total_work_threads=`
		`max_poll_threads=`
		`max_log_threads=`
		`max_notification_threads=`
		`max_request_threads=`
		`max_destroy_threads=`
		`max_ih_timer_threads=`

3	SpectroSERVER was experiencing stability issues when modeling a Tandberg Encoder device.	This was resolved by adding error checking to the code to check for NULL values and error messages.
4	SpectroSERVER performance was degraded when ATMClientApp models configured ATM links. The default configuration interval was set to 30 minutes and some external tables required 20 minutes to read due to their large size. The frequent reconfigurations caused a heavy load on the SpectroSERVER.	This was resolved by changing the default configuration interval to one day. In addition, if the attribute, `Create_Sub_Interfaces (11f3c)`, is set to "FALSE" the SpectroSERVER will turn off the timer that reconfigures ATM link models.
5	For Host_Compaq version 1.13, looping OIDs in the firmware created an endless loop in the read_next code because the end of table was NEVER reached. This caused memory growth and a SpectroSERVER crash.	This was resolved adding loop detection.

Toolkits

Corrected Issues: Toolkits

Item	Problem	Resolution
1	If a client program sent a CORBA invocation message of `CsRelationSrvc::testRelMTypeList()`, passing a list of `CsCModelType::CsCMTypeList` that contains an item or more of null pointers, the function `CsRelationSrvc::testRelMTypeList()` did not check if it was null or not. Instead, it assumed all items in the list were valid. For that reason, when a customer tried to pass a null pointer in the MTypeList to `CsRelationSrvc::testRelMTypeList()`, it caused the SpectroSERVER to crash.	This was resolved by ensuring that `CsRelationSrvc::testRelMTypeList()` throws a `VALUE_NULL` CORBA exception notifying the client program that it is sending a null pointer in the list.

Web Operator Suite

Corrected Issues: Web Operator Suite

Item	Problem	Resolution
1	While using Model Browser in WOS, the user clicked into Universe view and got the error: "The document contained no data. Try again later or contact the server's administrator". World and OrgChart views worked fine as did all other applications. This problem was directly related to the number of models in the view.	This was resolved by modifying the code to limit the number of requests made and store model names in a more efficient way to allow for larger number of models to exist in the view without causing any problems.

Known Anomalies in SPECTRUM 6.6 with Service Pack 5 CD Release

This section identifies known anomalies for SPECTRUM and its integrated applications in SPECTRUM 6.6 with Service Pack 5 CD release.

AR System Gateway

Known Anomalies: AR System Gateway

Item	Description	Solution
1	On Windows NT, if you modify filters when the Automatic Trouble Ticket Generator (`arsgated`) is running without SANM, the modifications are not recognized by the `arsgated`.	This issue will be corrected in a future release of SPECTRUM.
2	The Remedy password for the required SPECTRUM user is stored as a standard text value in the AR System Gateway resource file (.arsgrc). This value is not encrypted and could be cause for concern with regard to security. The Remedy API requires the password field in the ARControlStruct passed to ARVerifyUser to be "clear text" according to the Remedy Programmer's Guide: "The password for the specified user name, in clear text. The API encrypts this parameter before sending it to the server."	Ensure that permissions allow only appropriate individuals access to the .arsgrc file. **Note:** Make sure that the owner of the ARSGATED.PL, ARSGATED.DAEMON/EXE and ARS_CONFIG.PL have r/w permissions to this file or their respective operations will fail.

Enterprise Alarm Manager (EAM)

Known Anomalies: Enterprise Alarm Manager (EAM)

Item	Description	Solution
1	Newly created alarm descriptions in SpectroWATCH do not display in the Alarm Manager if the Alarm Manager was running when the watch and its custom alarm description were created. The alarm displays without a description of the new alarm.	Exit the Alarm Manager, then restart it. The new view updates to include the custom alarm description. This issue will be corrected in a future release of SPECTRUM.
2	When you run Alarm Manager (in a distributed environment) against a SpectroSERVER that does not have all model types linked, but is modeling another landscape where they are linked, these model types do not display in the Alarm Manager: Filter dialog's Model Type list. However, any alarms on models of those model types display in the alarm list.	Make sure the server that Alarm Manager is launched against has all model types (in the distributed environment) that need to display in the model type list.

Level I Developer's Toolkit

Known Anomalies: Level I Developer's Toolkit

Item	Description	Solution
1	When you run the MTE and import a MIB with an object name longer than 30 characters, you receive the following message, even when the object does not import: `The MIB was successfully imported.` In a terminal window or on the Control Panel, error messages display for MIB objects with names consisting of 30 or more characters that failed to import.	There are two workarounds: 1. The first is to identify each MIB object with 30+ characters in its name and shorten the name before running the MTE. 2. The second (for attributes with truncated group names) is to find the attributes that are listed as `no group` and manually assign the truncated group name in the Attribute View. If the MTE was run from the Control Panel, a list of MIB objects that did not import display on the Control Panel. If the MTE was run from the command line, a list of MIB objects that did not import display in that window. This issue will be corrected in a future release of SPECTRUM.

SpectroSERVER

Known Anomalies: SpectroSERVER

Item	Description	Solution
1	On the Windows NT/2000 server, the operating system is optimized to function as a file server by default. This causes the virtual memory system to assign precedence to the file cache when deciding which memory pages are eligible to be paged out. When large files are open, such as with SpectroSERVER and DDM databases, all of the available physical memory is assigned to the file cache. As available physical memory is allocated, SpectroSERVER, as well as other applications, have their executable code paged out in favor of maintaining the file cache. This results in poor application performance. In extreme cases, SpectroSERVER shuts down with a low memory error.	Change the default setting of the Windows paging algorithm using one of the following methods: *Windows NT Server* 1. Select **Control Panel** > **Network** > **Services** > **Server** > **Properties**. 2. Change property from **Optimize Throughput for File Sharing** to **Balance**. Windows 2000 Server 1. Select **Settings** > **Network and Dial-up Connections** > **Local Area Connections** > **Properties** > **File and Printer Sharing for Microsoft Networks** > **Properties**. 2. Change property from **Optimize Throughput for File Sharing** to **Balance**.

SPECTRUM Installation/Uninstallation Programs

Known Anomalies: SPECTRUM Installation/Uninstallation Programs

Item	Description	Solution
1	When you install SPECTRUM on Windows NT/2000 with a user name containing a space (for example, NT SPECTRUM) the installation appears to run successfully until the very end, then you receive a message similar to the following: `sed: Unterminated 's' command` You could possibly receive this message several times.	Avoid spaces in SPECTRUM user names.

Cabletron SmartSwitch 6000 Family

Management Module Information

MM Part Number	Device(s)	Firmware Version
SM-CSI1076	6E122-26, 6E123-26, 6E123-50, 6E128-26, 6E129-26, 6E132-25, 6E133-25, 6E133-37, 6E133-49, 6E138-25, 6E139-25 6E233-49	4.01.10
SM-CSI1082	6H122-08, 6H122-16, 6H123-50 6H128-08, 6H129-08, 6H133-37 6H202-24, 6H252-17	4.01.10 1.01.10 1.01.10
SM-CSI1088	6M146-04	4.01.10

Known Anomalies: Cabletron SmartSwitch 6000 Family

Item	Description	Solution
1	Attempts to create models of 6E123-50, 6H133-37, 6E138-25, or 6E128-26 devices via Model by IP or AutoDiscovery result in the models appearing as gen6000 devices. Attempts to model the 6E138-25 by Model Type result in the wrong model type alarm messages.	This is a firmware issue caused by incorrect SysObjectIDs being returned by the device.
2	In the Chassis Device view's Physical Application Display view for the 6E123-50 and 6H133-37, selecting the Port Display Form's **Speed** menu option, then selecting the Repeater Port Display Form's **Speed** menu option causes a value of `INV` (invalid) to appear for the ports.	The Port Display Form speed of 10 mb is correct. The Repeater Port Form **Speed** menu option is incorrect. This will be corrected in 7.0.

Cabletron SmartSwitch 9000/9500

Management Module Information

MM Part Number	Device(s)	Firmware Version
SM-CSI1030	9E13x-xx	2.06.10
SM-CSI1031	9F116-01	2.00.06
SM-CSI1032	9F1xx-xx, 9F2xx-xx	2.00.10
SM-CSI1035	9F4xx-xx 9F31x-xx	1.12.05 6.00.15 1.00.30
SM-CSI1036	9E3xx-xx, 9E4xx-xx	1.12.05
SM-CSI1038	9T122-xx 9T125-xx	1.08.07 1.02.17
SM-CSI1055	9E106-06	2.10.06
SM-CSI1059	9A128-01 9A426-xx	2.10.17 5.00.08
SM-CSI1066	9H42x-xx	1.12.05, 3.01.06
SM-CSI1073	9A656-04, 9A686-04	3.00.04
SM-CSI1074	9G42x-xx	1.12.05
SM-CSI1083	9T425-16, 9T428-16, 9T427-16	1.12.05
SM-CSI1092	9M426-02	2.01.02
SM-CSI1098	9E5xx-xx, 9G5xx-xx, 9H5xx-xx	1.02.09

Known Anomalies: SmartSwitch 9000/9500

Item	Description	Solution
1	9E42x-x and 9H42x-xx Transparent Bridging Port tables show no MIB-II interface statistics for INB interfaces for Port In Frames, Port Out Frames, and Port In Discards.	There are no plans to correct this issue.

Known Anomalies: SmartSwitch 9000/9500

Item	Description	Solution
2	You can create SmartSwitch 9000 models in Location or Organization views even though a Contains relation cannot be established with the SmartSwitch chassis model and the models do not show up in the Device view of the SmartSwitch.	Do not create SmartSwitch 9000 models in the Location or Organization views. Instead, create them in the Topology view and then copy the Device icon from the Universe Topology view into the Location view. The SmartSwitch chassis model has a Container view that contains Location view icons for all modeled SmartSwitch modules. This ensures that the proper relationship exists between the models.
3	When a 9A6x6 is modeled as a standalone device, the Chassis Device view incorrectly displays the backplane interfaces.	This is a firmware issue. Upgrade to firmware 3.00.04 or later.
4	The graph in the ATM Performance view may seem to display information incorrectly. For example, the Log and Lin (Linear) graphs may appear to show 100% of capacity when the cell rate exceeds a certain value.	This happens when the graph is used to show both percentages and rates, and has a limitation on the total cell rate the graph can show. Percentages cannot exceed 100% and the rates have a multiplier associated with them (noted by an asterisk next to the attribute). When the cell rate exceeds the graph's ability to show actual values, the % line appears flat on the graph. The actual tick-for-tick value of the rate is shown in the table beside the graph.
5	The 9H531-18 devices running firmware 01.07.11 model as 9H532_18 models.	The 9H531-18 and 9H532-18 devices use the same sysObjectID attribute. This is a firmware issue.

Cisco Catalyst

Management Module Information

MM Part Number	Device(s)	Firmware Version
SM-CAT1000	SwCat 1200	4.1, 4.21
SM-CAT1001	HubCat 1400	1.5
SM-CAT1002	HubCat 5xxx	2.1
SM-CAT1006	Catalyst 4xxx	NA
SM-CAT1008	Catalyst 85xx	NA

Known Anomalies: Cisco Catalyst

Item	Description	Solution
1	For SwCat1200 models, clicking either the Clear MAC or Clear Ports button in the CATStackApp model's Configuration view causes a SpectroGRAPH error message to display.	Use the read/write Community Name when modeling the device. This clears and sets all MAC and port counter attribute values to zero when you click the Clear Mac or Clear Ports button.
2	In the Device Topology view of the SwCat5505, reconfigured (swapped) boards appear in incorrect numeric order.	This is a firmware issue. The port information is correct. SPECTRUM reads the incorrect CATStackMib MIB values and cannot reorganize or update the interfaces in a logical order.
3	The Catalyst 8500 model does not display CAT_IF_Ports.	The device does not support the CISCO-STACK-MIB.
4	On Catalyst 4000 series devices, VLANs 1002-1005 show up as operational, but attempts to access them result in an Authorization Failure trap being sent by the device.	This is a firmware bug, documented in Cisco DDTS CSCea42364.

Cisco Router

Management Module Information

MM Part Number	Device(s)	Firmware Version
SM-CIS1001	Rtr_Cisco (Cisco Router 2) Rtr_CiscoIGS, CGS, AGS, MGS, 2500, 3000, 4000, 7000	11.1(8) 11.2
SM-CIS1002	Lightstream 10.10 (ATM Support)	11.2(5)/ wa3(2b)

Known Anomalies: Cisco Router

Item	Description	Solution
1	The CiscoView menu option and the CiscoView button in the Cisco Router management module do not work.	You must install the Ciscoview product and install the SPECTRUM integration available at: http://www.aprisma.com/partners/technology/cisco/NMSIntegration.shtml
2	Some Cisco device models let you enter any Community Name or none at all, which does not affect the model status; it stays green. However, if you remove an entered string, the model turns to the orange alarm state.	Cisco devices can be configured to respond to all SNMP requests without checking the Community Name.

Empire Agent

Management Module Information

MM Part Number	Device(s)	Firmware Version
SM-EMP1000	Empire Agent on Windows NT and Solaris systems	NA

Known Anomalies: Empire Agent

Item	Description	Solution

1	Some views may not display Message Queue table information and/or the values of the client attributes listed below, which are in the client NFS statistics and counters branch of the Empire proprietary MIBs.
	`clientNFSCalls`
	`clientNFSBadcalls`
	`clientNFSNclgets`
		The Message Queue table data display if the devices support Oracle (or other large database systems). The client attributes do not display due to a firmware issue.

2	Discovering TokenRingApp for a UNIX host device that has a Token Ring NIC causes unnecessary alarms on the device model.	This is a firmware issue. The Token Ring MIB objects fail some SNMP reads, which causes alarms to display. However, the device model returns to normal after one or two polls.

Enterasys Matrix E5

Management Module Information

MM Part Number	Device(s)	Firmware Version
SM-ENT1003	5C105, 5H102-48, 5H103-48, 5G106-06, 5 SSRM-02	1.03.00, 1.02.04

Known Anomalies: Enterasys Matrix E5

Item	Description	Solution
1	Autodiscovering 5H1xx and 5G1xx devices in a chassis creates Fanout connections rather than Pipes.	This is a firmware issue. The devices do not establish two-way communication through the backplane.

Extreme Devices

Management Module Information

MM Part Number	Device(s)	Firmware Version
SM-EXT1000	Extreme Summit switches	Summit ExtremeWare 2.1.7
	BlackDiamond 6808 Core switch	BlackDiamond: ExtremeWare 3.09b4 and version 5.0 for policy management
	Alpine 3808 Summit 48i	6.1.7 6.1.8

Known Anomalies: Extreme Devices

Item	Description	Solution
1	VLAN fault isolation is not supported for Extreme Summit switches running a version of ExtremeWare that is earlier than 6.0.	VLAN fault isolation requires the Extreme Vlan Stack Table, which is only supported in version 6.0 or higher. VLAN information is available via the ExtrVlanApp model in the Application view.
2	VLAN information may not be accessible from the VLAN List menu option in the Device Topology view.	VLAN information is available from the ExtrVlanApp model in the Application view. It is not available from the Device Topology view because VLAN information is not supported for Extreme Summit switches running a version of ExtremeWare earlier than 6.0.
3	AutoDiscovery connects an Alpine 3808 running firmware 6.1.7 and a Summit 48i running 6.1.8 using Extreme Discovery Protocol (EDP) but does not connect them to any non-Extreme devices.	For connection to non-Extreme devices from Extreme devices running these firmware versions, telnet to each device and enable the `dot1d` MIBs. Alternatively, you can upgrade the firmware to Extremeware 6.2 to use Extreme's proprietary MIB for connectivity.

F5 Networks

Management Module Information

MM Part Number	Device(s)	Firmware Version
SM-F5N1000	F5 Big-Ip Load Balancer	3.1.1

Known Anomalies: F5 Networks

Item	Description	Solution
1	The F5 Big-IP Load Balancer device model does not register trap events and alarms.	This is a firmware issue. The device does not properly implement the ipAddrEntry MIB table in compliance with RFC 2011.

ForeRunner Series of ATM Switches

Management Module Information

MM Part Number	Device(s)	Firmware Version
SM-FOR1000	ASX-100, ASX-200, 9A000, ASX-1000, ASX-4000	5.3.1

Known Anomalies: ForeRunner Series of ATM Switches

Item	Description	Solution
1	Yellow alarms occur if multiple ForeSystems workstations are modeled. The alarms only appear on ForeSystems workstation models using an older version of the ForeSystems ATM adaptor card.	Install a newer version of the ATM adapter card.

Host Compaq Module

Management Module Information

MM Part Number	Device(s)	Firmware Version
SM-CPQ1000	Host Compaq	NA

Known Anomalies: Host Compaq Module

Item	Description	Solution
1	The SNMP Agent Detail view does not show statistical information. Also, the view's Auth Traps field and the Detail view's Receive Breakdown and Transmit fields are enclosed by red boxes. If you change Auth Traps from `disabled` to `enabled`, an attribute error message appears.	This is a firmware issue. Compaq's SNMP2_Agent does not fully support MIB-II.

Juniper Networks

Management Module Information

MM Part Number	Device(s)	Firmware Version
SM-JPR1000	M5, M10, M20, M40, M40e, M160 Internet Backbone Routers	JUNOS 4.0R1.2

Known Anomalies: Juniper Networks

Item	Description	Solution
1	Juniper Internet JUNOS may incorrectly send OSPF traps (SNMP Version 1) with a non-standard, specific trap number between 9 and 24 when it should be between 1 and 16. As a result, the Juniper model shows these traps as `UNKNOWN` or displays the wrong event or alarm.	This firmware issue has been corrected by JUNOS 4.3.
2	Juniper Internet JUNOS may incorrectly send Juniper MPLS traps (SNMP Version 1) with a generic trap number of `0` when it should be `6`. As a result, the Juniper model shows these traps as `UNKNOWN`.	This firmware issue has been corrected by JUNOS 4.3.
3	Juniper Internet JUNOS 4.2 may not populate ifStackStatus OID `1.3.6.1.2.1.31.1.2.1.3`; therefore, sub-interfaces cannot be correctly mapped. All sub-interfaces appear in the Device Interface and Device Topology views.	This is an issue for firmware below JUNOS 5.2.

Packeteer PacketShaper

Management Module Information

MM Part Number	Device(s)	Firmware Version
SM-PKT1000	Packeteer Family	4.2.0

Known Anomalies: Packeteer PacketShaper

Item	Description	Solution
1	The Performance view displays incorrect load values.	This is a firmware issue.

Nortel Contivity Extranet Switch

Management Module Information

MM Part Number	Device(s)	Firmware Version
SM-NTL1004	Nortel Contivity Family	4.0.5

Known Anomalies: Nortel Contivity Extranet Switch

Item	Description	Solution
1	Red Boxes appear on the "IF Status Entry" and the "IF Configuration Entry" GIB views, even though all the information appears in the table entry.	This is an issue with firmware version 4.0.5 which incorrectly handles single reads with the instance supplied.

Riverstone SmartSwitch Router

Management Module Information

MM Part Number	Device(s)	Firmware Version
SM-RST1000	RS-32000, 38000, 8600, 8000, 3000, 2100, 2000 IA-1100, 1200	8.0.0.8

Known Anomalies: Riverstone SmartSwitch Router

Item	Description	Solution
1	Riverstone SmartSwitch Routers configured with MPLS boards running firmware 8.0.0.8 incorrectly report the operational status as `down` and the administrative status as `off` for port interfaces that are configured to be operational.	This issue does not occur in firmware 8.0.2.0. You can ping these routers with the IPs of the target interfaces; then when you telnet to each router, you will see those interfaces are configured to be operational (`up` and `on`).

SmartSwitch Routers (SSR)

Management Module Information

MM Part Number	Device(s)	Firmware Version
SM-CSI1091	SSR 32000, 8600, 8000, 3000, 2100, 2000, 1200, and IA-1100	NA
SM-ENT1005	X-Pedition 8600, 8000, 2100, 2000, and ER16	NA
SM-RST1000	RS 32000, 8600, 8000, 3000, 2100, 2000, 1200, and IA-1100	NA
SM-ENT1001	6-SSRM-02	NA
SM-TRN1000	BE2xx, TL1000, and TLGateway	NA

Known Anomalies: SSR

Item	Description	Solution
1	The Port Performance view for the SSR 8000 incorrectly displays the in_error and error_rate values as `100%`. The values should be zero when no connection exists.	This is a firmware issue.
2	When an SSR device with firmware 3.0 is modeled via router discovery, connections to interfaces on the SSR do not resolve.	Manually model the connections to each router.
3	Serial interfaces for the SSR 8600 incorrectly show `10000000` for the `ifSpeed`.	This is a firmware issue.
4	The Chassis view does not display port or chassis models for devices running firmware 8.0.1.0.	This is a firmware issue.

Sun Management Center Agent

Management Module Information

MM Part Number	Device(s)	Firmware Version
SM-SUN1000	Workstations and servers supported by the Sun Management Center Agent	3.0

Known Anomalies: Sun Management Center Agent

Item	Description	Solution
1	The fields in some SPECTRUM views that support the MIB-II SNMP group may not display any values. For example, this could happen in the Performance Detail view.	Sun provides two versions of MIB-II support with the Agent. One version, called MIB-II System (which loads automatically), only supports the System, Interface, and IP groups. A second version, called MIB-II Instrumentation (which requires a license key), is part of the Advanced Systems Monitoring package and supports the System, Interface, IP, ICMP, TCP, and UDP groups. Sun's MIB-II support for the Sun Management Center Agent is a change from their default agent, snmpdx, which seems to support all MIB groups in MIB-II.
2	The mechanism for changing the Community Name on a Sun Management Center (SMC) workstation does not function properly. Only the Community Name supplied during model creation can be used to communicate with the SMC.	This issue has been reported to Sun.

SynOptics 5000 Hubs

Management Module Information

MM Part Number	Device(s)	Firmware Version
SM-SYN1003	53xx Enet, 55xx TR, 59xx FDDI	1.5.1, 1.5.1, 2.2.6

Known Anomalies: SynOptics 5000 Hubs

Item	Description	Solution
1	SynOptics only counts good frames when monitoring Ethernet traffic. As the number of frames with errors goes up, the number of good frames goes down. This directly affects the Load value in the Port, Segment, Cluster, and Attachment Performance views.	This is an agent issue. Users must evaluate the %Errors in the Performance views and know that when the %Errors goes up, the load displayed does not reflect the actual load on the Ethernet segment.
2	Traps are only generated against the IP address of the first Data Collection Engine (DCE) on an Ethernet or Token Ring Network Management Module (NMM). If contact is lost with the first DCE, you do not receive traps.	This is a firmware issue.
3	In the Device view, Token Ring DCE icons can disappear and the NMM menu options change to their defaults, Module Notes and Module Configuration.	This is a firmware issue. When the Token Ring NMM is rebooting, its entry can disappear from the device's module table.
4	Information deleted from the Config File Name and/or Image File Name fields in the DCE Agent Configuration view reappears in the view after the view's next poll cycle.	This is a firmware issue. Replace the entries to be deleted with null characters or blank spaces.
5	In the Ring In/Ring Out Extension Information view, the Ring In UNA and Ring Out UNA can be `0.0.0.0.0.0` or both values can be the same.	This is a firmware issue.

Known Anomalies: SynOptics 5000 Hubs

Item	Description	Solution
6	Attempts to change all Module Ring Attachments and the Module Ring Speed for all attachments in a Token Ring Module Configuration view fail when done simultaneously during the editing session.	This is a firmware issue. Change the Module Ring Attachments then change the Module Ring Speed (or vice versa). Do not try to change both at the same time.

SynOptics Modules

Management Module Information

MM Part Number	Device(s)	Firmware Version
SM-SYN1001	HubSyn3FDDI (SynOptics 3000)	5.1.0
SM-SYN1002	HubSynEnet28xx (SynOptics 28xx)	5.3.1
SM-SYN1004	SynOptics 332xS (Enet Bridge)	1.0.0
SM-SYN1005	SynOptics 39xx (FDDI)	2.0.48
SM-SYN1006	SynOptics 28xxx	2.0.3
SM-SYN1008	HubSyn27xx (SynOptics 27xx)	5.11
SM-SYN1009	HubSyn29xx (SynOptics 29xx)	2.2.4

Known Anomalies: SynOptics Modules

Item	Description	Solution
1	Inaccurate statistics can appear in the SynOptics Port Performance view.	This is a firmware issue.

Wellfleet Routers

Management Module Information

MM Part Number	Device(s)	Firmware Version
SM-WEL1003	Wellfleet Router 2	NA

Known Anomalies: Wellfleet Routers

Item	Description	Solution
1	The DCLI ports on the Rtr_Bay_Wflet do not model appropriately when you migrate SPECTRUM from any 5.0rev1 release or higher to any 6.X release. This is because the attribute `Create_Sub_Interfaces` is set to `FALSE` by default on the earlier releases. When migrating to 6.X releases, the default value is preserved.	Do the following to set the `Create_Sub_Interfaces` attribute to `TRUE`: 1. Select the **Redundancy/Discovery** button in the **Configuration** view to display the **Redundancy/Discovery Control** view. 2. Toggle Create Sub Interfaces to `TRUE` and select **File** > **Save All Changes**.

Multiple Management Modules

Note: Ignore fields enclosed in red boxes or error messages warning of blank table entries. These indicate that the required data was not obtainable from the device, and they occur when the device firmware does not support these data requests from SPECTRUM.

Known Anomalies: Multiple Management Modules

Item	Description	Solution
1	On some model types, SPECTRUM does not recognize manual changes to environmental variables until the SPECTRUM Control Panel is shut down and reopened. For example, this is true with CIMPATH when used to launch Compaq Insight Manager, ROAMEXCPATH when used to launch an application for RoamAbout, CVIEW when used to launch Cisco Works on some Cisco devices, and COPPEREXCPATH when used to launch Copper View Element Manager for Copper Mountain devices.	Restart the SPECTRUM Control Panel after making this type of change.
2	Some read/write attributes in RFC1315App can not be changed on some device models.	Some manufactures do not implement all of the attributes from RFC1315 as read/write, as is specified by the standard, but rather as read-only. This can cause errors when trying to write to these attributes, as writing to them is prohibited by the firmware.

Discontinued Products and Components

This section identifies the discontinued products and components for the SPECTRUM 6.6 with Service Pack 5 CD release, relative to the 6.5.1 release.

About Discontinued Products and Components

Aprisma is continually reviewing the products that it supports to ensure that they are still in use and in line with the product strategy set forth for the company. When it is determined that a product or component is no longer being actively utilized by a large set of our customer base, the determination is made as to whether or not Aprisma will continue to develop, test, and support that product. This continual review and resulting discontinuation effort allows Aprisma to ensure that valuable resources are being applied and utilized to develop, test, and support existing and new areas of the functionality that reflects the most current and actively used areas.

Below, please find a listing of those products and components that are being discontinued with the SPECTRUM 6.6 with Service Pack 5 CD release. In addition, please see the recommended migration path details where they exist. The recommended migration path indicates the solution that should be implemented by the customer if they wish to replace functionality provided by products or components to be discontinued.

Device Management Components

This section describes any general (or vendor specific) device management capabilities that are no longer supplied with SPECTRUM.

Cabletron Device Management Components

There is no known migration path for replacing these capabilities, however Enterasys Networks may offer software to accomplish these Device/Element Management tasks for Cabletron devices.

The following Cabletron Device Management components are no longer available as part of SPECTUM.

- Buttons in Device Configuration views and Search Manager menu picks which previously launched the following components have been removed: Community Names (cscmunty) / Community Table (cscmtytb); TFTP Download (cstftpdl)
- Alarm Configuration (e5alarms, r2al, r3al, r4al)
- Broadcast Suppression, System Resources, Frame Priorities, MAC Priorities, Port Priorities, Port Redirection (spmawin)
- Front Panel Redundancy (fpred)
- Link/Seg Traps (r2hwtr, r3hwtr, r4hwtr)
- Port Source Address (r4sap)
- Ring Map (e5map)
- Security, Security Configuration, Repeater Security (e5sec/r4sec)
- Source Addressing (r4sa)
- Statistics (e5stats)
- Trap Table (traptbl)
- WAN Configuration (wancon)

The SEHI Management module no longer includes Device Chassis and Device Chassis Physical views.

Management Modules

Table 1 shows discontinued management modules and the recommended migration path. Discontinuation is effective November 15, 2002.

Table 1: Discontinued Management Modules

Discontinued Part Number	Part Number Description	Recommended Migration Path
SM-ATT1000	AT&T Smart Hub	Generic SNMP Module
SM-CAY1001	Cayman GatorBox, GatorMIM, or GatorStar devices running firmware version 2.2	Generic SNMP Module
SM-CHP1002	3Com CoreBuilder 5000 and Online hubs	Generic SNMP Module
SM-CIS1001	Cisco Routers: IGS, CGS, AGS, MGS, 2500, 3000, 4000, and 7000	Rtr_Cisco
SM-CSI1028	Cabletron Distributed LAN Monitor	N/A
SM-SYN1007	SynOptics' SNMP-managed Distributed 5xxx Ethernet series Network Management Modules (NMMs), Host Modules and Chassis	Generic SNMP Module
SM-UNB1001	Ungermann-Bass Access/One hubs.	Generic SNMP Module

Questions & Answers

Why is Aprisma discontinuing these Management Modules?

Aprisma has determined that due to the age of the devices to be managed with these management modules, as well as the small number of customers who are actively using them, the above list of Management Modules will be discontinued by Aprisma.

What is the recommended migration path?

For all of the discontinued Management Modules listed in the above graph, customers will be encouraged to migrate to the Generic SNMP module (or the specific module listed) if they wish to continue managing the affected devices.

What assistance is provided to upgrade customers from these discontinued Management Modules to the Generic SNMP Module?

Customers will be required to complete any migration work themselves (as discussed in the SPECTRUM Installation Guide) or enlist the help of Aprisma Professional Services to complete the work. The Installation Guide

and migration process have been significantly enhance in 6.6 SP2, to ease this transition.

How long will orders be accepted for these Management Modules?

Orders for these Management Modules will no longer be accepted after October 15th, 2002.

How will support be handled on these Management Modules?

For current maintenance customers, phone support will be provided on the product for one year after the date of discontinuation. Therefore, phone support will be provided until 11/15/2003. For non-maintenance customers, support will be provided on a per incident, time and materials cost basis until 11/15/2002. Please note that support will be limited to troubleshooting the current software components to the best of our ability through product support.

Feature Comparison

Table 2 compares the features of each discontinued management module (MM) with the features of the recommended replacement product.

Table 2: Discontinued MM Feature Comparisons

Discontinued Product	Recommended Replacement	Feature Comparison
SM-ATT1000	Generic SNMP Module	• Device Chassis view will be removed. • Hub Configuration, Self Test, Download, and Security views will be removed. • ATT_Chassis App will be removed. • ATTPort will be replaced by Gen_IF_Ports
SM-CAY1001	Generic SNMP Module	• CaymanRptrApp will be removed.

Table 2: Discontinued MM Feature Comparisons

SM-CHP1002	Generic SNMP Module	• Device Chassis view will be removed. • Power Management, Device Configuration, Chassis Configuration, and Interface Configuration views will be removed. • CComGenBdgApp will be replaced by Gen_Bridge_App • CComPort are no longer modeled. The following applications will be removed: • CComBdgPtApp • CComCBaseTApp • CComChas42App • CComChasApp • CComLASMApp • CComMonitorApp • CComPktChanApp • CComSecureApp • CComSlaveApp • CComSpTreeApp • CComTopLvlApp • CComTransp_App • CComTRMonApp • CComTrnkApp • CComTRSlaveApp • CComRMONXApp • CComGenBdgApp
SM-CIS1001	Rtr_Cisco	• No noticeable changes.
SM-CSI1028	N/A	• N/A

Table 2: Discontinued MM Feature Comparisons

SM-SYN1007	Generic SNMP Module	• Syn5DNComApp will be removed. • Syn5DNEnetApp will be removed. • Syn5DNComApp will be removed. • Syn5DNEnetApp will be removed. • GnSNMPDev discovers SNMP2_Agent. • GnSNMPDev discovers RMONApp.
SM-UNB1001	Generic SNMP Module	• UB_Bridge_App will be replaced by Gen_Bridge_App • UBGnPort are no longer modeled. • UBHubApp will be removed. • UB_TPL_App will be removed. • UB_TRTier_App will be removed. • UB_Trap_App will be removed. • UB_Firmw_App will be removed. • UB_EWA_App will be removed.

EPI, SSAPI, IHAPI, Simulator Playback Tool

Table 3 shows discontinued Level II Toolkits and the recommended migration path. Discontinuation is effective November 15, 2002.

Table 3: Discontinued Level II Toolkits

Discontinued Part Number	Part Number Description	Recommended Migration Path
ST-LEGACY, ST-CSI1004	Level II Toolkits: External Protocol Interface (EPI)	ST-Corba
ST-LEGACY, ST-CSI1005	Level II Toolkits: SpectroSERVER API (SSAPI)	ST-Corba
ST-LEGACY, ST-CSI1006	Level II Toolkits: Inference Handler API (IHAPI)	None
ST-LEGACY	Level II Toolkits: Simulator Playback Tool	None

Questions & Answers

Why is Aprisma discontinuing EPI, SSAPI, IHAPI, and the Simulator Playback Tool?

These products are the development toolkits for the SPECTRUM legacy APIs. The legacy APIs have been replaced with Spectrum's CORBA interface. The CORBA interface will allow customers and partners to develop applications using standards based development environments (Java, C++). Our research has shown that very few of our current customers are using these toolkits; as such the decision was made to simplify the development options and only offer support for CORBA moving forward.

What is the recommended migration path?

Please see the Feature Comparison [page 78] to gain a better understanding of the functionality that will be available in the recommended product.

If you have previously created an integration utilizing the EPI, SSAPI, or IHAPI toolkits, and wish to continue utilizing the integration, please contact SPECTRUM Product Management at product_management@aprisma.com.

Is there a formal program to upgrade customers from EPI, SSAPI, IHAPI, and the Simulator Playback Tool to the recommended migration product?

There is not a formal program to migrate either the tools or the resulting work they have been used to complete to the newly recommended products. Customers will be required to complete any migration work themselves or enlist the help of Aprisma Professional Services to complete the work.

How long will orders be accepted for EPI, SSAPI, IHAPI, and the Simulator Playback Tool?

Orders for EPI, SSAPI, IHAPI, and the Simulator Playback Tool will no longer be accepted after October 15th, 2002.

How will support be handled on EPI, SSAPI, IHAPI, and the Simulator Playback Tool?

If you have previously created an integration utilizing the EPI, SSAPI, or IHAPI toolkits, and wish to continue utilizing the integration, please contact SPECTRUM Product Management at product_management@aprisma.com**.**

For current maintenance customers, phone support will be provided on the product for one year after the date of discontinuation. Therefore, phone support will be provided until 11/15/2003. For non-maintenance customers, support will be provided on a per incident, time and materials cost basis until 11/15/2002. Note that support will be limited to troubleshooting the current software components to the best of our ability through product support.

Feature Comparison

Table 4 compares the features of discontinued products with the features of recommended replacement products.

Table 4: Discontinued Level II Toolkit Feature Comparisons

Discontinued Product	Migration Path	Comparison
ST-CSI1005 - SpectroSERVER API (SSAPI)	ST-Corba	All functionality available to the customer or partner currently developing applications for SPECTRUM using the SSAPI interface is available in the ST-Corba toolkit. If you have previously created an integration utilizing the EPI, SSAPI, or IHAPI toolkits, and wish to continue utilizing the integration, please contact SPECTRUM Product Management at product_management@aprisma.com.
ST-CSI1004 - External Protocol Interface (EPI)	ST-Corba	The ST-Corba toolkit provides the developer the ability to develop an external application to create SPECTRUM events based on proprietary event streams. If you have previously created an integration utilizing the EPI, SSAPI, or IHAPI toolkits, and wish to continue utilizing the integration, please contact SPECTRUM Product Management at product_management@aprisma.com.
ST-CSI1006 - Inference Handler API (IHAPI)	None	No replacement is available for this functionality. If you have previously created an integration utilizing the EPI, SSAPI, or IHAPI toolkits, and wish to continue utilizing the integration, please contact SPECTRUM Product Management at product_management@aprisma.com.
ST-LEGACY – Simulator Playback Tool	None	No replacement is available for this functionality.

SpectroRX

Discontinuation is effective November 15, 2002.

Discontinued Part Number	Part Number Description	Recommended Migration Path
SA-SPECTRORX	SpectroRX	None

Questions & Answers

Why is Aprisma discontinuing SpectroRX?

Due to the lack of customers utilizing this product, it was determined that this product would be discontinued.

What is the recommended migration path?

There is no migration path for users of SpectroRX. Therefore, Aprisma is unable to provide a customer currently using SpectroRX with any alternate solutions that would allow them to continue to fulfill requirements that are currently being met with this product.

Is there a formal program to upgrade customers from SpectroRX to the recommended migration product?

There is no formal program to upgrade customers from this product because there is no recommended migration product.

How long will orders be accepted for SpectroRX?

Orders for SpectroRX will no longer be accepted after October 15th, 2002.

How will support be handled on SpectroRX?

For current maintenance customers, phone support will be provided on the product for one year after the date of discontinuation. Therefore, phone support will be provided until 11/15/2003. For non-maintenance customers, support will be provided on a per incident, time and materials cost basis until 11/15/2002. Note that support will be limited to troubleshooting the current software components to the best of our ability through product support.

Feature Comparison

There is no migration path for users of SpectroRX, and therefore there is no features comparison available.

Support for Export to SAS, Ingress, Sybase, Oracle, and Microsoft SQL Database Types

The following table shows discontinued support and the recommended migration path. Discontinuation is effective November 15, 2002.

Discontinued Functionality / Support	Recommended Migration Path
Support for Export to SAS, Ingress, Sybase, Oracle, Microsoft SQL Database Types	Export to Ascii

Questions & Answers

Why is Aprisma discontinuing support for Export to SAS, Ingress, Sybase, Oracle, and Microsoft SQL Database Types?

It was determined, based on Aprisma product strategy research showing that the additional data types are not in use by a large portion of our customer base and the migration path options available for our customers, that support for the above mentioned database types will be discontinued by Aprisma.

What is meant by discontinued functionality/support?

Discontinued functionality/support refers to specific functionality and/or operating platform for Aprisma product that will no longer be supported. Specifically, Aprisma will no longer support the export of data to SAS, Ingress, Sybase, Oracle, or Microsoft SQL database types. We will instead, only support the export of data to the standard Ascii data type. Additionally, the options to export to these other data types will be removed from the SPECTRUM product in Version 6.6 and above.

Moving forward, no fixes or enhancements will be made to the product to enhance or maintain capabilities to export data to the alternate data types. In addition, Aprisma will no longer complete testing to ensure export to alternate data types is functioning appropriately.

What is the migration path?

Customers will be encouraged to export to Ascii instead.

Is there a formal program to train customers on the Export to Ascii?

There is no formal program to train customers on the recommended migration path. Customers will be wholly responsible for managing any required changes.

How will support be handled on Export to SAS, Ingress, Sybase, Oracle, and Microsoft SQL database Types?

For current maintenance customers, phone support will be provided on this functionality for one year after the date of discontinuation. Therefore, phone support will be provided until 11/15/2003. For non-maintenance customers, support will be provided on a per incident, time and materials cost basis until 11/15/2002. Please note that support will be limited to troubleshooting the current software components to the best of our ability through product support.

Feature Comparison

The following table compares the discontinued support with the recommended replacement.

Discontinued Functionality / Support	**Migration Path**	**Comparison**
Support for Export to SAS, Ingress, Sybase, Oracle, Microsoft SQL database Types	Export to Ascii	Ascii is an industry standard format that can easily be converted by the customer to the database types that will no longer be supported by Aprisma. Customers are encouraged to export to Ascii and utilize conversion tools available from the appropriate database vendors to import the data in Ascii format into the desired database format type.

Support for Netscape

The following table shows the discontinued product and the recommended migration path. Discontinuation is effective November 15, 2002.

Discontinued Functionality / Support	Recommended Migration Path
Support for Netscape	Internet Explorer Version 5.x and above

Questions & Answers

Why is Aprisma discontinuing support for NetScape?

Based on Aprisma's Product Strategy, focusing on developing on and supporting only one Browser type will allow Aprisma to develop more robust web solutions at a faster pace.

What is meant by discontinued functionality/support?

Discontinued functionality/support refers to specific functionality and/or operating platform for Aprisma product that will no longer be supported. Specifically, Aprisma will no longer support Web Operator Suite running on the Netscape platform. We will instead, only support Web Operator Suite operating on Internet Explorer Version 5.x and higher.

> **Note:** This applies to the client only. The WOS Apache Web Server can still be run on the Solaris platform. It is the client that requires IE 5.x or above.

Moving forward, no fixes or enhancements will be made to the product to enhance or maintain the products' capability to operate Web Operator Suite on Netscape. In addition, Aprisma will no longer complete testing to ensure that Web Operator Suite works appropriately when running on Netscape.

What is the migration path?

Users who access Web Operator Suite should access it from a Windows machine moving forward.

Is there a formal program to move customers to Internet Explorer 5.x or above?

There is no formal program to move customers to Internet Explorer 5.x or above. Customers will be responsible for managing this change themselves.

How will support be handled on Netscape?

For current maintenance customers, phone support will be provided on this platform for one year after the date of discontinuation. Therefore, phone support will be provided until 11/15/2003. For non-maintenance customers, support will be provided on a per incident, time and materials cost basis until 11/15/2002. Note that support will be limited to troubleshooting the current software components to the best of our ability through product support.

Feature Comparison

The following table compares the features of the discontinued product with the features of the recommended replacement product.

Discontinued Functionality / Support	**Migration Path**	**Comparison**
Support for Netscape	Internet Explorer	Internet Explorer is an industry leading Browser provider. While Aprisma is not prepared to provide a feature comparison of Internet Explorer to Netscape, we have every confidence that a functionality comparison would prove comparable capabilities between the two.

Index

Numerics

1G582-09 [21]
1G694-13 [21]
1H582-25 [21]
1H582-51 [21]
3Com [20]
3Com40x0 [20]
3Com44xx [20]
3Com49xx [20]
4050 [20]
4060 [20]
4095 [20]
4400 [20]
4900 [20]
4900SX [20]
53xx Enet [66]
9A656-04 [52]
9A686-04 [52]
9E106-06 [52]
9E423-xx [52]
9F12x-xx [52]
9F426-02 [52]
9M426-02 [52]
9T12x-xx [52]
9T425-16 [52]

A

Acedirector [25]
Alteon [25]
ASX-100 [59]
ASX-200 [59]
AutoDiscovery [12], [13]

B

Brocade [25]

C

Cadent C4 [21]
Catalyst 4503 [20]
Catalyst 4506 [20]
Catalyst 4507R [20]
Cisco [20], [21], [23], [25]
Cisco VPN Client 3002 [23]
Cisco VPN Client 3005 [23]
Cisco VPN Client 3015 [23]
Cisco VPN Client 3030 [23]
Cisco VPN Client 3060 [23]
Cisco VPN Client 3080 [23]
Cisco3xxxVPN [23]
Contivity 100 [22]
Contivity 1000 [23]
Contivity 1010 [23]
Contivity 1050 [23]
Contivity 1100 [23]
Contivity 1500 [23]
Contivity 1600 [23]
Contivity 1700 [23]
Contivity 200 [22]
Contivity 2000 [23]
Contivity 2500 [23]
Contivity 2600 [23]
Contivity 2700 [23]
Contivity 400 [22]
Contivity 4000 [23]
Contivity 4600 [23]
Contivity 600 [23]
ContivityVPN [23]
ContivityVPNII [22]
Corrected and Known Anomalies-Management Modules
  Cabletron SmartSwitch 6000 Family [51]
  Cabletron SmartSwitch 9000/9500 [52]
  Cisco Catalyst [54]
  Cisco Router [55]
  Empire Agent [56]
  Enterasys Matrix E5 [57]
  Extreme Devices [58]
  F5 Networks [59]
  ForeRunner Series of ATM Switches [59]
  Host Compaq Module [60]
  Juniper Networks [61]
  Nortel Contivity [62]

Packeteer PacketShaper [62]
Riverstone SmartSwitch Router [63]
SmartSwitch Router (SSR) [64]
Sun Management Center Agent [65]
SynOptics 5000 Hubs [66]
SynOptics Modules [67]
Wellfleet Routers [68]
Corrected and Known Anomalies-SPECTRUM
AR System Gateway [47]
Enterprise Alarm Manager (EAM) [48]
Level I Developer's Toolkit [49]
SpectroSERVER [50]
SPECTRUM Installation Program [50]

E

Enterasys [21], [22], [24]

F

Fault Management [17]

H

HubSyn27xx [67]
HubSyn29xx [67]

J

JMibTools [13]

M

MPLS Manager [18]
Mulitcast Manager [19]

P

Process Daemon [26]

R

RoamAbout R2 [24]
RoamAboutR2 [24]

S

Service Performance Manager [26], [27]
SM [72]
SM-CAT1000 [54]
SM-CAT1001 [54]
SM-CAT1002 [54]
SM-CAT1008 [54]
SM-CAY1001 [72]
SM-CHP1002 [72]
SM-CIS1001 [55], [72]
SM-CIS1002 [55]
SM-CSI1028 [72]
SM-CSI1030 [52]
SM-CSI1031 [52]
SM-CSI1032 [52]
SM-CSI1035 [52]
SM-CSI1036 [52]
SM-CSI1038 [52]
SM-CSI1055 [52]
SM-CSI1059 [52]
SM-CSI1066 [52]
SM-CSI1073 [52]
SM-CSI1074 [52]
SM-CSI1076 [51]
SM-CSI1082 [51]
SM-CSI1083 [52]
SM-CSI1088 [51]
SM-CSI1091 [64]
SM-CSI1092 [52]
SM-CSI1098 [52]
SM-EMP1000 [56]
SM-ENT1001 [64]
SM-ENT1003 [57]
SM-ENT1005 [64]
SM-EXT1000 [58]
SM-F5N1000 [59]
SM-FOR1000 [59]
SM-GHO1004 [60]
SM-JPR1000 [61]
SM-NTL1004 [62]

SM-PKT1000 [62]
SM-RST1000 [63], [64]
SM-SUN1000 [65]
SM-SYN1001 [67]
SM-SYN1002 [67]
SM-SYN1003 [66]
SM-SYN1004 [67]
SM-SYN1005 [67]
SM-SYN1006 [67]
SM-SYN1007 [72]
SM-SYN1008 [67]
SM-SYN1009 [67]
SM-TRN1000 [64]
SM-UNB1001 [72]
SM-WEL1003 [68]
SPECTRUM Reporting Gateway [27]
SPM [27]
Sun Fire B1600 [22]
SunFireSw [22]
SynOptics [67]
SynOptics 332xS [67]
SynOptics 39xx [67]

T

TR NMM [66]

V

Vanguard [26]

W

Wellfleet Router II [68]
Windows NT [60]

X

XSR-1805 [22]
XSR-1850 [22]